TASK ORDER (TO)

GSQ0016AJ0009

Enterprise Operations and Security Services (EOSS)

in support of:

The Army National Guard (ARNG)

Issued to:
SRA International, Inc.

issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405

April 2015

FEDSIM Project Number AR00702

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

NOTE: The Section numbers in this Task Order (TO) correspond to the Section numbers in the Alliant Contract. Section B of the contractor's Alliant Contract is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

B.1 GENERAL

The work shall be performed in accordance with (IAW) all Sections of this TO and the contractor's Basic Contract, under which the resulting TO will be placed. An acronym listing to support this Task Order Request (TOR) is included in **Section J, Attachment G**.

B.5 CONTRACT ACCESS FEE

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a Contract Access Fee (CAF). The amount of the CAF is ¾ % (i.e., (.0075)) of the total price/cost of contractor performance. This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO award. CAF is capped at $100,000 per contract year.

B.6 ORDER TYPES

The contractor shall perform the effort required by this TO on a:

a. Cost-Plus-Award-Fee (CPAF) basis for CLINs:
   1. 0001, 1001, 2001, 3001, 4001

b. Optional CPAF basis for CLINs:
   1. 0002a, 1002a, 2002a, 3002a, 4002a
   2. 0002b, 1002b, 2002b, 3002b, 4002b
   3. 0002c, 1002c, 2002c, 3002c, 4002c

c. Firm-Fixed-Price (FFP) basis for CLINs:
   1. 0003, 1003, 2003, 3003, 4003

d. Cost Reimbursable Not-to-Exceed (NTE) basis for CLINs:
   1. 0004, 1004, 2004, 3004, 4004
   2. 0005, 1005, 2005, 3005, 4005
   3. 0006, 1006, 2006, 3006, 4006

e. Not-to-Exceed (NTE) basis for CLINs:
   1. 0007, 1007, 2007, 3007, 4007

B.7 ORDER PRICING (ALL ORDER TYPES)

Long-distance travel is defined as travel over 50 miles from ARNG's Readiness Center, Arlington Hall, 111 South George Mason Drive, Arlington, VA 22204 and/or the contractor-provided COCO facility. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CLIN	Contract Line Item Number
FFP	Firm Fixed Price
CPAF	Cost Plus Award Fee
NTE	Not-to-Exceed
ODC	Other Direct Cost

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

B.7.1 BASE PERIOD: 12 MONTHS

MANDATORY LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
0001	Labor – Tasks 1, 2, 4, 5, 7	(b) (4)		

OPTIONAL LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
0002	Labor – Task 6	(b) (4)		
0002a	Task 6 – Labor (**DO NOT include labor for move to GOCO)**			
0002b	Reserved			
0002c	Reserved			

FIRM FIXED PRICE CLIN

CLIN	Description	QTY	Unit	Total Firm Fixed Price
0003	Accounting for Contractor Services – Task 8	1	1	(b) (4)

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total NTE Price
0004	Long Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
0005	Tools Including Indirect Handling Rate (b) (4)	NTE	
0006	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total NTE Price
0007	Contract Access Fee	NTE	(b) (4)

TOTAL BASE PERIOD CLINs: (b) (4)

B.7.2 FIRST OPTION PERIOD: 12 MONTHS

MANDATORY LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
1001	Labor – Tasks 1, 4, 5, 7	(b) (4)		

OPTIONAL LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
1002	Labor – Task 6	(b) (4)		
1002a	Task 6 – Labor (**DO NOT include labor for move to GOCO)**			
1002b	Reserved			
1002c	Reserved			

FIRM FIXED PRICE CLIN

CLIN	Description	QTY	Unit	Total Firm Fixed Price
1003	Accounting for Contractor Services – Task 8	1	1	(b) (4)

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total NTE Price
1004	Long Distance Travel Including Indirect Handling Rate _(b) (4)	NTE	(b) (4)
1005	Tools Including Indirect Handling Rate _(b) (4)	NTE	
1006	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total NTE Price
1007	Contract Access Fee	NTE	(b) (4)

TOTAL OPTION PERIOD 1 CLINs: (b) (4)

B.7.3 SECOND OPTION PERIOD: 12 MONTHS

MANDATORY LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
2001	Labor – Tasks 1, 4, 5, 7	(b) (4)		

OPTIONAL LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
2002	Labor – Task 6	(b) (4)		
2002a	Task 6 – Labor (**DO NOT include labor for move to GOCO)**			
2002b	Reserved			
2002c	Reserved			

FIRM FIXED PRICE CLIN

CLIN	Description	QTY	Unit	Total Firm Fixed Price
2003	Accounting for Contractor Services – Task 8	1	1	(b) (4)

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total NTE Price
2004	Long Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
2005	Tools Including Indirect Handling Rate (b) (4)	NTE	
2006	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total NTE Price
2007	Contract Access Fee	NTE	(b) (4)

TOTAL OPTION PERIOD 2 CLINs: (b) (4)

B.7.4 THIRD OPTION PERIOD: 12 MONTHS

MANDATORY LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
3001	Labor – Tasks 1, 4, 5, 7	(b) (4)		

OPTIONAL LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
3002	Labor – Task 6	(b) (4)		
3002a	Task 6 – Labor (**DO NOT include labor for move to GOCO)**			
3002b	Reserved			
3002c	Reserved			

FIRM FIXED PRICE CLIN

CLIN	Description	QTY	Unit	Total Firm Fixed Price
3003	Accounting for Contractor Services – Task 8	1	1	(b) (4)

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total NTE Price
3004	Long Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
3005	Tools Including Indirect Handling Rate (b) (4)	NTE	
3006	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total NTE Price
3007	Contract Access Fee	NTE	(b) (4)

TOTAL OPTION PERIOD 3 CLINs: (b) (4)

B.7.5 FOURTH OPTION PERIOD: 12 MONTHS

MANDATORY LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
4001	Labor – Tasks 1, 4, 5, 7	(b) (4)		

OPTIONAL LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
4002	Labor – Task 6 and 3	(b) (4)		
4002a	Task 6 – Labor (**DO NOT include labor for move to GOCO)**			
4002b	Move to GOCO			
4002c	Task 3 – Transition-Out			

FIRM FIXED PRICE CLIN

CLIN	Description	QTY	Unit	Total Firm Fixed Price
4003	Accounting for Contractor Services – Task 8	1	1	(b) (4)

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total NTE Price
4004	Long Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
4005	Tools Including Indirect Handling Rate (b) (4)	NTE	
4006	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CONTRACT ACCESS FEE (Capped at $100,000 per period)

CLIN	Description		Total NTE Price
4007	Contract Access Fee	NTE	(b) (4)

TOTAL OPTION PERIOD 4 CLINs: (b) (4)

GRAND TOTAL ALL CLINs: **$247,355,568**

B.12 SECTION B TABLES

B.12.1 INDIRECT/MATERIAL HANDLING RATE

Long-Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate IAW the contractor's disclosed practices.

a. If no indirect/material handling rate is allowable IAW the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
b. If no rate is specified in the basic contract, no indirect rate shall be applied to or reimbursed on these costs.
c. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.12.2 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing Alliant contract labor categories.

B.12.3 CONTRACTOR ACCOUNTING FOR CONTRACT SERVICES

The costs to be reported under this CLIN are those associated with the reporting requirements specified in **Section C.5.8** and they relate to this TO only.

B.13 INCREMENTAL FUNDING

B.13.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of $16,490,000 for CLINs 0001 and 0004 through 0006 is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs will be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through April 25, 2016, unless otherwise noted in **Section B.7**. The TO will be modified to add funds incrementally up to the maximum of $246,855,568 over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

Incremental Funding Chart for CPAF

The Incremental Funding Chart is a separate Excel spreadsheet. It must be completed at award and included in the awarded TO as an Attachment in **Section J**. See detailed instructions in the Excel spreadsheet.

See **Section J, Attachment D**- Incremental Funding Chart (Excel Spreadsheet).

B.14 AWARD FEE PLANNED VALUE/RESULTS REPORTING TABLE

Award Fee Results will be recorded in the Award Fee Planned Value/Results Reporting Table located in Section 4.2 of the AFDP (see **Section J, Attachment D**). The AFDP must be finalized post-award and maintained throughout the life of the TO to reflect results and plan changes from period-to-period. Each time the plan changes, the updated plan should be incorporated in the TO through modification.

The Award Fee Determination Plan (AFDP) establishes award fee. See **Section J, Attachment E** – Award Fee Determination Plan (Word document).

SECTION C –PERFORMANCE WORK STATEMENT

C.1 BACKGROUND

The Army National Guard (ARNG) requires support for the operation, modernization, expansion, and further evolution of the Enterprise Operations and Security Services (EOSS) program and the associated Information Technology (IT) services, infrastructure support, and program management services. The EOSS program supports the ARNG enterprise information technology (IT) infrastructure, its Wide Area Network (WAN) and the associated services. EOSS uses the Information Technology Infrastructure Library (ITIL®) best practices framework as the basis for IT service management model. The EOSS service model is the mechanism that ARNG uses to provide management, operations, maintenance, security, and support for the IT and telecommunications infrastructure that provide enterprise data, voice, and video networks. The EOSS program manages all circuits, network nodes, supporting equipment, and software. Taken together, these provide Command, Control, Communications, and Computers (C4) support across the ARNG. The EOSS model encompasses the strategies, acquisition, operation, and disposition of all the hardware and software resources necessary to provide IT and communications support, including the GuardNet Non-Secure Internet Protocol Router Network (NIPRNet) WAN and GuardNet-S Secret Internet Protocol Router Network (SIPRNet) WAN.

EOSS was established in 2006 with the goal of moving ARNG's IT operations from a traditional organizational and operational model based on separate support structures to an integrated lifecycle support framework that emphasizes proactive operational planning and analysis that supports the ARNG mission needs. EOSS supports IT service management across large geographical areas implementing and utilizing the ITIL v3 framework to manage IT operations. Some of the major support requirements are: network operations management, audio and video conferencing, distance learning classroom, user authentication and authorization, Boulete, Moores, and Cloer (BMC) Information Technology Service Management (ITSM), network and IT engineering, asset management/Government-Furnished Equipment (GFE) maintenance and disposition, SIPRNet, Information Assurance, Certification and Accreditation (C&A), Alternate site/Disaster Recovery (DR)/Continuity of Operations (COOP) operations, and secure facilities. These services are managed across the 50 states, the District of Columbia, and the territories of Guam, Puerto Rico, and the Virgin Islands.

C.1.1 PURPOSE

The purpose of this requirement is to acquire contractor support for the operations, modernization, expansion, and further evolution of the EOSS program and the associated IT services for the ARNG. The contractor shall provide a wide range of IT and infrastructure support, and program management services for EOSS that will be described in the task requirements. It is the intent of the ARNG to migrate the current infrastructure to the JIE construct in accordance with (IAW) the Draft JIE Implementation Plan (See **Section J, Attachment Y**).

C.1.2 AGENCY MISSION

C.1.2.1 ARMY NATIONAL GUARD (ARNG)

The ARNG is a military force with Federal and state missions that range from providing emergency assistance to state and local law enforcement agencies to supporting the nation's military strategies. It is a unique and complex organizational and operational environment involving the National Guard Bureau (NGB), the ARNG, and various directorates. There are National Guard entities located throughout the 50 states, Puerto Rico, Virgin Islands, Guam, and the District of Columbia. The National Guard is unique in that by law it has a dual mission: 1) to support the Governors under Title 32 United States Code (USC) Section 502(f), and 2) to provide a high state of preparedness and be available on short notice to the President under Title 10 USC. Under Title 10, the National Guard units fall under control of the Army command structure.

C.1.2.2 ARNG G6 - CHIEF INFORMATION OFFICE

The Chief Information Office of the ARNG (ARNG G6) (the requiring activity) helps preserve the operational ARNG in three ways. Firstly, by developing and maintaining operational and tactical networks. Secondly, the ARNG G6 governs, develops, and integrates all applications and systems. Thirdly, the ARNG G6 leverages other DoD IT solutions to meet ARNG requirements.

Figure 1 below illustrates the channels of communication between the Secretary of Defense and the Adjutants General of the 50 states, the three territories, and the District of Columbia. The ARNG G6 enables the unique capability to provide seamless communications across state and Federal boundaries, between Title 10 and Title 32 missions. Importantly, the ARNG G6 facilitates the nation's force of choice for domestic operations by providing interoperability with state, territorial, tribal, and local governments by enabling rapidly deployable forces for Governors and Northern Command in support of homeland missions. See **Section J, Attachments S and T** for organizational chart for the G6 and for the Information Networks Division (IMN).

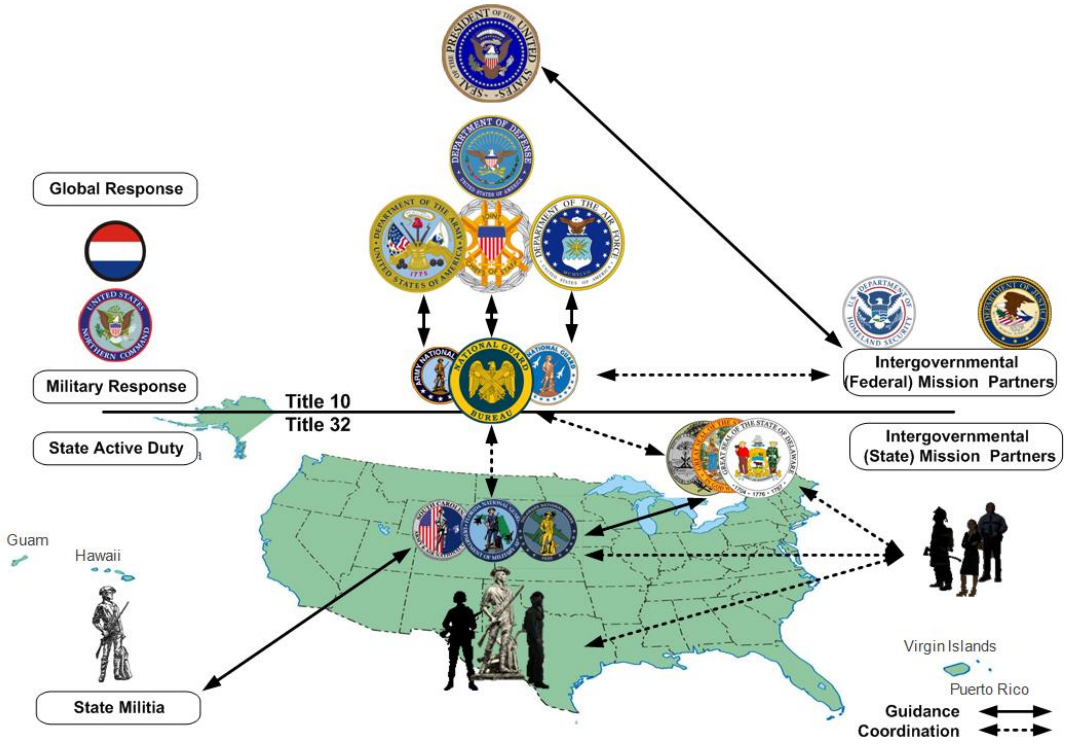

Figure 1. GuardNet Stakeholders

C.2 SCOPE

The EOSS program supports the ARNG enterprise IT infrastructure, its WAN and the associated services. EOSS uses the ITIL best practices framework as the basis for IT service management model. The contractor shall perform the following:

a. Operate the GuardNet and GuardNet-S networks and maintain delivery of GuardNet and GuardNet-S networks and computing services.
b. Support the GuardNet and GuardNet-S networks and associated computing services from requirement identification to service disposal.
c. Ensure continued security of the network and proactive enhancement of Information Assurance (IA) capabilities to meet evolving and emerging threats.
d. Provide support for Government Command and Control (C2), i.e. provide communication with the 54 sites (50 states, the District of Columbia, and three territories), to ensure flexible and responsive operation and defense of the network.
e. Leverage Department of Defense (DoD) enterprise security services provided by the Defense Information Systems Agency (DISA) to meet user requirements as technically and fiscally feasible and approved by the Designated Approving Authority (DAA) as defined by the future JIE architecture.
f. Maintain continuity of service when primary support systems operate in degraded mode at Camp Robinson in Arkansas or other alternate site as per COOP.

Very little long-distance travel is required to support the requirements of this TOR. Most interaction by the contractor with the states and COOP sites is performed remotely from the Regional Cyber Center-National Guard (RCC-NG) formally known as Network Operations Security Center (NOSC). The RCC-NG is currently a contractor-provided facility.

The contractor shall interface with other contractors, internal and external to the ARNG, and shall ensure that the IT operations adhere to required ARNG IT security policies and procedures.

All equipment supplied by the contractor shall be Energy Star compliant IAW FAR Clause 52.223-15 in **Section I** of the TOR.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

The National Guard and its components depend on a wide variety of assets to deliver services. Serving as the backbone of the IT infrastructure is a WAN that is known as GuardNet. The GuardNet Enterprise is composed of two elements: 1) an Enterprise layer that is a Multiprotocol Label Switching (MPLS) network providing the communications channel for voice, video, and data among all National Guard entities, and 2) state-level enclaves that provide data communications for the state-level ARNG units. The communication channels from the ARNG's end-points (GuardNet Enterprise layer) along with the network's core are provided by a third party under the Networx contract (Verizon) administered by the United States (U.S.) GSA. This point of presence, using the Verizon contract, must be provided with the contractor-provided facility. The contractor shall manage all the edge devices (routers, firewalls, etc.) on the Enterprise side of the GuardNet network. These devices are owned by ARNG.

The contractor shall provide real-time (mostly remotely from the RCC-NG), interactive support across Continental United States (CONUS) and Outside the Continental United States (OCONUS) locations for the GuardNet network. The contractor shall maintain the interoperability of the network with other components of the Army, other Military Services, and coalition partners. These communication channels are maintained by DISA.

GuardNet delivers enterprise services and network connectivity among the 54 Joint Forces Headquarters (JFHQ), other DoD networks, and DISA. However, there are additional functions in the Management Layer associated with operating GuardNet (e.g., monitoring vendor service levels for this TO, traffic shaping, and managing security infrastructure).

ARNG Enterprise Network

The ARNG G6 maintains and operates ARNG enterprise IT systems, including the GuardNet and GuardNet-S WANs, Active Directory (AD), Video and Audio conferencing, and other systems. The ARNG Network Division (ARNG-IMN) of the ARNG G6 has direct responsibility for ARNG Enterprise network operations and for managing the EOSS TO. The EOSS TO provides resources for the operation and maintenance of the ARNG enterprise IT networks.

Enterprise Operations and Security Services (EOSS)

The EOSS service model is the mechanism that ARNG uses to provide management, operations, maintenance, security, and support for the IT and telecommunications infrastructure that provide enterprise data, voice, and video networks. The framework emphasizes proactive operational planning and analysis supporting ARNG mission needs.

The EOSS program manages all circuits, network nodes, supporting equipment, and software. Taken together, these provide C4 support across the ARNG. The EOSS model encompasses the strategies, acquisition, operation, and disposition of all the hardware and software resources necessary to provide IT and communications support, including the GuardNet/GuardNet-S wide area networks. The EOSS program includes the following services:

a. Enterprise Service Desk for the GuardNet/GuardNet-S WANs and the associated IT operations.
b. GuardNet/GuardNet-S WAN RCC-NG.
c. Enterprise AD design and management of the root and selected lower-level objects.
d. Engineering services for generally defined IT and network operations.
e. Video and audio conference support.
f. Information assurance protection and the security of all GuardNet/GuardNet-S and Enterprise IT elements.
g. Higher-level support to units managing state-level enclaves.
h. Support planning for future JIE implementation.

GuardNet

GuardNet/GuardNet-S is defined to be the WAN infrastructure of the National Guard which securely supports the NGB Joint team using nationwide information systems as a mission-command network. GuardNet/GuardNet-S supports tactical and force-generating operations every day. The GuardNet mission is to "Provide a secure, robust, and dynamic telecommunication infrastructure consolidating voice, data, and video services for the States, Territories, and the District of Columbia in one integrated network."

This network spans 15 time zones and is at 2,385 separate locations. GuardNet provides ARNG access to the Army's LandWarNet (LWN) and Joint access to Air Force network (AFNet) services in those states. The network supports approximately 130 applications and video to 400 endpoints, and links across all CONUS and OCONUS armories and other facilities for data transmittal between the Department of the Army, the NGB, and the ARNG sites.

By using GuardNet/GuardNet-S the states, territories, and the District of Columbia can connect to the NIPRNet and SIPRNET defense networks operated by DISA. From NIPRNet, GuardNet end-users can access the Internet. Security devices exist at connections between the Federally controlled Enterprise (Title 10) and state-controlled enclave (Title 32) portions of GuardNet, between the Federally controlled portion of GuardNet and DISA's network, and between DISA's network and the Internet.

The GuardNet Enterprise provides two connections (Primary and Alternate) to every state and other sites, resulting in over 110 Service Delivery Points (SDPs). The Primary and Alternate sites are interconnected via the state's internal network. At the time of solicitation, all circuits use DS3 or higher access with bandwidth adjusted to meet traffic demand. The WAN provider is responsible for delivery of data to the ARNG-managed routers.

A GuardNet SDP at each JFHQ contains the demarcation point between GuardNet Enterprise and the state enclave. The ARNG's RCC-NG manages the GuardNet side of the demarcation point and the state's Director of Information Management (DOIM/J6/G6) is responsible for managing the state's network. The demarcation between GuardNet Distributed Learning Program (DLP) classrooms is located on the side of Enterprise Top Level Architecture (TLA), which secures the DLP traffic with perimeter firewall and Intrusion Protection System (IPS)/Intrusion Detection System (IDS). The GuardNet topology diagram in **Section J, Attachment U** shows equipment, connections, and interrelationships.

A GFE hardware inventory and a software list of those items to be used and managed by the contractor, can be found in **Section J, Attachment V**. The inventory shows the GFE hand receipt at the RCC-NG. The contractor shall manage all GuardNet configuration items not just those listed on the hand receipt.

C.4 OBJECTIVE

ARNG G6 intends to continue a high level of operational performance and further develop the EOSS concept of delivering services in a manner consistent with the ITIL service management framework and that meets the following specific objectives:

a. Increase operational efficiencies of the available resources through increased use of ITIL processes resulting in improved Total Cost of Ownership (TCO).
b. Improve customer service and internal efficiency by emphasizing proactive system management using ITIL processes.
c. Position the ARNG's EOSS program as the premier source of IT and communications services for the National Guard.
d. Provide IT operations and support to the ARNG states as the Enterprise Service Provider.
e. Provide real-time continuous security and configuration monitoring of systems in agreement with National Institute of Standards and Technology (NIST) SP 800-137 to improve security of the ARNG systems.
f. Develop service delivery pricing models and basis.
g. Lower TCO for ARNG enterprise operations.

C.5 TASKS

The contractor shall support the following tasks in accordance with (IAW) the Government's Service Level Agreements (SLAs):

Task 1: Task Order Program Management

Task 2: Transition-In
Task 3: Transition-Out (optional)
Task 4: IT Service Management
Task 5: Managed Services
Task 6: Project and Initiative Support (optional)
Task 7: Technical Refresh Support
Task 8: Accounting for Contract Services

The contractor shall supply a contractor-owned contractor operated (COCO) facility to provide a Network Operations Center (NOC)/ Security Operations Center (SOC) and ancillary support that also provides sufficient space for the Government to monitor activities and conduct review meetings. This facility will be referred to as the RCC-NG in this document. It shall be located within a 15 mile radius of ARNG's Readiness Center located at 111 South George Mason Drive, Arlington, VA and it shall meet the facility criteria contained in **Section J, Attachment LL** to include meeting DHS FSL Level II regulations at a minimum. The majority of contractor-supplied work in support of this effort shall occur at this facility. It is the intent of the Government to require the Contractor to move to a Government facility within the life of this Task Order.

In compliance with U.S. Office of Management and Budget (OMB) guidance dated 28 September 2010, Federal agencies are required to ensure that procurements of networked information technology comply with Federal Acquisition Regulation (FAR) requirements for using the U.S. Government version 6 (USGv6) profile and testing program for the completeness and quality of Internet Protocol version 6 (IPv6) capabilities.

The contractor shall ensure that all equipment and software proposed and/or provided by the contractor is compatible with the above stated guidance.

All references to Contract Data Requirements Lists (CDRLs) are the standards for content and format to be applied to the referenced deliverables.

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this TO. The contractor shall provide a Program Manager (PM) as a primary point of contact who shall provide management, direction, administration, quality control, and leadership of the execution of this TO. The contractor shall schedule meetings and provide deliverables IAW the Government-approved delivery schedule. The contractor shall establish and maintain a formal program management organization IAW **CDRL 01** Program Management Plan (PMP) and provide the Government with an organization diagram and a directory of the positions, names, and contact information of all engineering, operations, and program management personnel who are designated as Government points of contact.

C.5.1.1 SUBTASK 1 - PERFORMANCE MANAGEMENT

The EOSS TO is a performance-based contract under which ARNG will rate the contractor according to the performance criteria defined in the SLAs/SLOs for Tasks 2, 4, 5, 6, and 7. The Government will establish am Award Fee Determination Plan (AFDP) (**Section J, Attachment E**) that incorporates the SLAs established under the EOSS TO. The Government will use the AFDP as a basis for evaluating contractor performance in a systematic way.

The contractor shall be responsible for gathering, processing, and presenting the SLA data at the regularly scheduled review session.

This solicitation defines the end user of the EOSS services as the user seeking assistance from the EOSS program. From the contractor‘s point of view, the customer is the ARNG, which in turn provides services to its own customers (end users).

The contractor shall:

a. Deliver EOSS services IAW SLAs (**CDRL 02**) established under the EOSS TO.
b. All SLAs (**CDRL 02**) must be met no later than (NLT) the end of the Transition-in period. As services are transitioned from the out-going contractor to the incoming contractor, the in-coming contractor shall be responsible for meeting the SLAs for the corresponding service. The objective is to refine previous EOSS SLAs, define appropriate new SLAs, and implement ongoing performance-based metrics against these objectives iteratively over the life of the Task Order with a first set of SLAs in place NLT 120 days after contract start. This will be outlined in the SLA (**CDRL 02**) and reported in the Monthly Program Status Report (MPSR).
c. Employ ITIL-based service level management processes and monitor and report on service management levels throughout the period of performance.
d. Provide personnel, tools, and processes to monitor, manage, and regulate performance and security and continuously optimize performance.
e. Develop a Quality Control Plan (QCP) as part of the PMP that describes the overall plan, procedures, and controls that the contractor will use to provide and maintain a satisfactory quality system for the duration of the period of performance.
f. Capture and convert information from assigned components and systems to generate the performance measurements required by the EOSS SLAs.
g. Conduct regular service review meetings to report on service levels and end-to-end performance.
h. Identify required improvements in service levels on a continual basis.
i. Develop and maintain an Integrated Master Schedule (IMS) (**CDRL 04**) (**Section F, Deliverable 01**) that is vertically traceable to the contractor’s Work Breakdown Schedule (WBS) and the requirements of the Performance Work Statement (PWS). All schedule requirements must be contained in the IMS. The IMS shall contain critical path information about all on-going projects and synchronize their relationship to other projects and activities. The contractor shall evaluate the impact of new initiatives or proposed changes to ongoing project activities and develop recommendations as to

acceptance of this new project and consequences of such decision on the on-going EOSS and related activities and plans and report in the review boards.

C.5.1.2 SUBTASK 2 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting (**Section F, Deliverable 02**) at the location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include vital contractor personnel, representatives from the directorates, other relevant Government personnel, and the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR). The contractor shall provide the following at the Kick-Off Meeting:

a. Transition-In Plan
b. Status on the Completion of the Draft Project Management Plan (PMP)
c. Status on the Completion of the Final Quality Control Plan (QCP)
d. Earned Value Management (EVM) Plan

C.5.1.3 SUBTASK 3 – EMPLOY EARNED VALUE MANAGEMENT (EVM)

The contractor shall employ and report on EVM in the management of this TO. See **Section H.19**, Earned Value Management**,** for the EVM requirements.

C.5.1.4 SUBTASK 4 – CONVENE TECHNICAL STATUS MEETINGS

The contractor PM shall convene a monthly Technical Status Meeting (**CDRL 03**) (**Section F, Deliverable 03**) with the Technical Point of Contact (TPOC), COR, and other vital Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MPSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

C.5.1.5 SUBTASK 5 – PREPARE A PROGRAM MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP **(CDRL 01)**. The PMP shall:

a. Describe the proposed management approach.
b. Include milestones, tasks, and subtasks required in this TO.
c. Develop and maintain an IMS (**CDRL 04**) that is vertically traceable to the contractor Work Breakdown Structure (WBS), and the requirements of this PWS. All schedules required throughout the contract must be contained in the IMS. This IMS shall contain

critical path information about all on-going projects and synchronize their relationship to other projects and activities.

d. Provide for an overall WBS and associated responsibilities and partnerships between or among Government organizations.
e. Include the contractor's QCP and EVM Plan
f. Provide methods used to meet the Government's SLAs and reporting results.
g. Provide methods for improving service level management and operating more efficiently, including proactive, ITIL-compliant service enhancements and problem avoidance.
h. Provide methods for maintaining relationships with other contractor supporting or using EOSS services.
i. Provide methods for developing metrics/Key Performance Indicators (KPIs).

The contractor shall provide the Government with a Draft PMP (**Section F, Deliverable 04**), on which the Government will make comments. The contractor shall provide a Final PMP (**Section F, Deliverable 05**) that incorporates the Government's comments. The PMP is an evolutionary document that shall be updated annually at a minimum IAW **CDRL 01**.

C.5.1.6 SUBTASK 6 – STATUS REPORTS

C.5.1.6.1 SUBTASK 6.1 – DAILY STATUS REPORT

The contractor shall submit Daily System Status Report (Reports **CDRL 05**) (**Section F, Deliverable 06**) with input from the Service Operations staff. The Daily System Status Report is an informal means of working with Service Operations and communicating information about:

a. System performance.
b. Status of current and upcoming events and activities.
c. Events that may have an impact on operations.

C.5.1.6.2 SUBTASK 6.2 – WEEKLY STATUS REPORT

The contractor shall submit the Weekly System Status Report (**CDRL 05**) (**Section F, Deliverable 07**) with input from the each of the functional areas. The Weekly System Status Report shall provide information about the current state of the operations as well as planned activities. This report information shall be structured into the following sections.

a. Service Level Management
b. Incidents and Problems
c. Changes
d. Maintenance
e. Projects Status
f. Contractual Activities
g. Issues

C.5.1.6.3 SUBTASK 6.3 – MONTHLY PROGRAM STATUS REPORT (MPSR)

The contractor shall develop and provide a Monthly Program Status Report (MPSR) (**CDRL 05**) (**Section F, Deliverable 08**) using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the TPOC and the COR. See the Sample MPSR in **Section J, Attachment B**. The MPSR shall include the following:

a. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MPSR for the reporting period).
g. EVM statistics.
h. Accumulated invoiced cost for each CLIN up to the previous month.
i. Projected cost of each CLIN for the current month.
j. Service Level Management statistics.
k. Availability Management statistics.
l. Capacity Management statistics and progress.
m. Demand Management statistics.
n. Incident, Request, and Trouble Ticket Summary.
o. Service Desk Summary.
p. Change Management activities.
q. Maintenance activities.
r. Updated risk analysis.
s. Other contractor activities.

C.5.1.7 SUBTASK 7 – PREPARE TRIP REPORTS

The Government will identify the need for a contractor Trip Report (Reports **CDRL 05**) (**Section F, Deliverable 09**) when the request for travel is submitted. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, point of contact (POC) at travel location, summary and conclusions, and any items for further actions (action items). The contractor shall format IAW Army Regulation 25-50 “Preparing and Managing Correspondence.”

C.5.1.8 SUBTASK 8 – UPDATE QUALITY CONTROL PLAN (QCP)

The contractor shall update the QCP submitted with its proposal and provide a Final QCP (**Section F, Deliverable 10**). The contractor shall periodically update the QCP as changes in program processes are identified.

C.5.1.9 SUBTASK 9 – PERFORM RISK MANAGEMENT ACTIVITIES

The contractor shall actively manage risks and its mitigation plans/strategies for the EOSS TO across all service management areas. In particular, the contractor shall perform the following:

a. Establish and execute a risk management program IAW the Risk Management Guide for DoD Acquisition, Sixth Edition (Version 1.0), August 4, 2006, and document the program in the Risk Management Plan (**CDRL 06**) (**Section F, Deliverable 11**).

    1. Lay out the organizational structure that will support risk management by identifying planning responsibilities, mapping them to contractor staff, identifying the ARNG staff dependencies, and presenting the schedule for performing and completing this work.
    2. Using a Responsible, Accountable, Consulted, Informed (RACI) matrix approach, define personnel roles, responsibilities and accountability for executing the risk management plan and monitoring performance, map these responsibilities to contractor staff, and identify interfaces to the ARNG staff.
    3. Define the lifecycle management risk mitigation process.
    4. Define controls that the contractor will use to minimize risk to the operations.
    5. Address the risks associated with changes to the existing infrastructure, introduction of new elements into the infrastructure as well as external factors, such as technology trends and changing business environment.

b. Conduct a risk analysis (e.g., risk identification and assessment) and brief results to the Government on a regular basis.
c. Schedule, attend, provide input to, and manage monthly risk management meetings.
d. Update the status of existing and new contractor risks for inclusion in the MPSR (**CDRLs 03 and 05**).
e. Prepare and present new program risks with proposed mitigation plans and strategies and report on the mitigation status of existing risks.
f. Integrate the risk management processes with the IT service management processes in conformance with ITIL best practices.

C.5.1.10 SUBTASK 10 – PROVIDE IT GOVERNANCE

ARNG G6 has established IT Governance organizations, policies, and procedures. These IT Governance activities directly impact the execution and management of the EOSS program.

The contractor shall:

a. Actively participate in IT Governance organizations as requested by ARNG.
b. Develop strategies and plan recommendations that support the management of IT services for the ARNG Enterprise system.
c. Enforce ARNG IT Governance strategies, policies, and plans as they apply to the implementation and management of EOSS services.

C.5.1.11 SUBTASK 11 – MAINTAIN GUARDKNOWLEDGEONLINE (GKO) DOCUMENTATION LIBRARY

ARNG G6 needs to maintain a complete and up-to-date set of all deliverables and documentation provided under the EOSS TO.

The contractor shall:

a. Use GKO (SharePoint) as the document library.
b. Ensure that this library contains up-to-date versions of all deliverable documents produced by the contractor or directed for inclusion by the ARNG.
c. Maintain permission-based access, including user-level restriction of access to data elements and functions that one can perform against these elements.
d. Populate, update, and maintain current the content of the Documentation Library.

C.5.1.12 SUBTASK 12 – PREPARE AND MAINTAIN STANDARD OPERATING PROCEDURES (SOP)

After the transition period, the contractor shall prepare and deliver any contractor-recommended SOPs (**Section F, Deliverable 12**) associated with the required tasks of this TOR. The Government will review the recommended SOPs and provided the final Government-approved set for project use. Based on Government direction, the contractor shall update the SOPs as procedures change and report these changes with the MPSR.

C.5.2 TASK 2 – TRANSITION-IN

The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall provide a Final Transition-In Plan (**Section F, Deliverable 14**) that will be based on the contractor's proposal Transition-in Plan, within five calendar-days of Project Start. All transition activities shall be completed 120 calendar days after Project Start. If the contractor is not able to establish SIPRNet connectivity within the required 120 days due to Government delay, the contractor shall notify the Government sufficiently in advance of the deadline such that the Government can provide temporary SIPRNet access using the capability in the RCC and still remain within the 120-day requirement. The contactor can utilize all existing GuardNet infrastructure during transition as long as risks are appropriately mitigated.

The contractor shall begin implementation of its Transition-In Plan NLT five calendar days after Project Start. The contractor shall perform IAW the Transition-in SLAs/SLOs contained in **Section J, Attachment MM**.

C.5.3 TASK 3 – TRANSITION-OUT (OPTIONAL)

The contractor shall provide a Transition-Out Plan (**CDRL 07**) (**Section F, Deliverable 15**) that facilitates the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan NLT 120 calendar days after the Government exercises the Transition-out option and shall update the Plan as necessary reflecting current operations and service levels and provide these updates at the appropriate MPSR. The contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge to include the following:

a. Project management processes.
b. Points of contact.
c. Location of technical and project management documentation, data, and methods of providing these to the incoming service provider.
d. Status of ongoing technical initiatives.
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel.
g. Schedules and milestones.
h. Actions required of the Government.
i. Methods of measuring transition risks that includes a complete inventory of transition risks with assigned severity and probability, and response plans to address the risks either through avoidance, mitigation, or other means.
j. Method of permitting the successor service provider to observe and become familiar with any and all operations specified in this TOR for a minimum of 120 calendar days prior to the expiration or termination of the TO.
k. Method of establishing and maintaining effective communication with the incoming service provider for the period of the transition via weekly status meetings.
l. Detail knowledge transfer including the following:

    1. Methods for ensuring that all information assets and related configuration information is up-to-date and available for the Government's review at least 120 calendar days prior to the end of the TO. As part of the Plan the contractor shall:

        A. Deliver to IMN electronic copies of all Government data and information stored in the contractor's systems in the format requested by IMN within 15 workdays from the IMN request.
        B. Turn over all administrative access information, i.e., user-name and password, to the ARNG at least 90 calendar days prior to the end of the TO.

C. Provide process descriptions and detailed procedures for all systems management and support processes and update as necessary during the transition-out.

2. Method for adherence to the approved Transition-Out Plan once phase-out activities are initiated.
3. Method for conducting a joint contractor and Government inventory of GFE and contractor-furnished equipment (CFE) and all operational, engineering, procedural, educational, and any other documentation and presentations produced as part of delivering EOSS services within ten workdays of an IMN request.
4. Method for certifying that all Government information has been purged from any contractor-owned system used to process Government information.

The contractor shall implement the requirements of the Government-approved Transition-Out Plan at the direction of the Government in support of transitioning to a new service provider.

C.5.4 TASK 4 - IT SERVICE MANAGEMENT

The contractor shall apply and adapt the best practices for IT service management (ITSM) as the basis for managing and operating the ARNG's IT enterprise. ITSM provides a structured approach for managing the EOSS services. The contractor shall implement ITSM practices IAW the ITIL best practices framework 2011 that provides guidance to service providers on the provision of quality IT services and on the processes, functions, and capabilities needed to support them. The ARNG has adopted ITIL as its service management model and expects to further develop and mature the ITIL practices and processes, with assistance from the contractor, that have been implemented under EOSS.

The objectives of implementing ITIL under the EOSS TO are the following:

a. Be responsible for all process in the service delivery framework that promotes the consistent delivery and management of the EOSS Services to end users.
b. Focus on the delivery of services to end users.
c. Respond to dynamic mission requirements and priorities.
d. Implement new processes and technologies, and improve current processes.
e. Realize cost efficiencies through the use of well-defined, repeatable, and well-documented processes to manage IT systems and services throughout the lifecycle.

The contractor shall update, enhance, and maintain an IT Service Management Plan (**CDRL 08**) (**Section F, Deliverable 13**) describing the Service Management System how ITSM will be managed, supporting policies, and the overall service delivery. This federated plan will build from current EOSS plans that outline the processes, roles, and responsibilities, associated technologies, and SLA/Service Level Objectives (SLOs) tied to each of the ITIL Lifecycles including the following sub-sections:

1. Continual Service Improvement

2. Service Strategy
   A. Service Portfolio Management
   B. Technology Planning/Strategy Management
   C. Financial Management
3. Service Design
   A. Project Design and Coordination
   B. Service Catalog Management
   C. Service Level Management
   D. Supplier Management
   E. Availability Management
   F. Capacity Management.
   G. IT Service Continuity
   H. Information Security Management
4. Service Transition
   A. Project Transition Management
   B. Service Asset and Transition
   C. Change Management
   D. Release & Deployment Management
   E. Knowledge Management
   F. Service Validation and Testing
5. Service Operations
   A. Event Management
   B. Incident Management
   C. Request Management
   D. Problem Management
   E. Access Management

C.5.4.1 SUBTASK 1 - CONTINUAL SERVICE IMPROVEMENT (CSI)

The contractor shall continually monitor and evaluate EOSS services, processes, and technologies to determine effectiveness and efficiency and whether they address ARNG business objectives. CSI interacts with all areas of IT service delivery and all stages of the ITSM framework, Service Strategy, Service Design, Service Transition, and Service Operations. CSI includes ensuring continuous quality improvements and identifying a means of improving delivery of services. Implementation of CSI practices, which objectively measure the contractor's and EOSS program's ability to deliver EOSS services and develop a means of applying proactive capacity and availability management techniques are key in EOSS service delivery.

The contractor shall:

a. Implement and manage the ITIL seven-step improvement process for CSI.
b. Develop and maintain a CSI Register (**CDRL 09**) (**Section F, Deliverable 17**) to capture and track Service Improvements and measure proposed benefits with realized ones as well as process improvement initiatives, timelines, capabilities, and costs reflective of the Government business priorities and mission needs.
c. Conduct service and process assessment review and/or meetings.
d. Design and periodically update a Baseline Service and Process Assessment Report to measure effectiveness and efficiency (**CDRL 05**) (**Section F, Deliverable 16**).
e. Coordinate the design and improvement of measurements, metrics, benchmarking, KPIs, and reporting methods with Service Level Management and Service and Process Owners.
f. Coordinate with Service Operations activities to ensure current tools and other measurement methods are available in production and have the capacity for proposed service and process measurements and they provide the correct measurements.
g. Suggest new tools and measurement methods and coordinate on their deployment.
h. Develop Service Improvement Plans in coordination with Service Design to introduce SI changes into the production environment and determine the appropriate resourcing.
i. Coordinate CSI training with Knowledge Management.
j. Report CSI activities in the MPSR.

C.5.4.2 SUBTASK 2 - SERVICE STRATEGY

Service Strategy focuses on aligning IT services with the needs of business. It describes the processes, procedures, tasks, and checklists used by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of performance. It allows the organization to establish a baseline from which it can plan, implement, measure, and improve services, processes, and technologies. The contractor shall perform the following subtasks in support of Service Strategy.

C.5.4.2.1 SUBTASK 2.1 SERVICE PORTOFOLIO MANGEMENT

The contractor shall manage and enhance ARNG-IMN's Service Portfolio including introducing new services (Service Pipeline), ensuring current services (Service Catalog) meeting current requirements, and retiring services no longer required. These services and support shall conform to the most current Army Command, Control, Communication, Computers Information Management (C4IM) services list. The current Enterprise IT Services and Support Portfolio is included in **Section J, Attachment X**.

C.5.4.2.2 SUBTASK 2.2 - TECHNOLOGY PLANNING

ARNG is actively engaged in developing long-range plans for delivery of IT services to its current and future customer base with JIE Architecture and future End-State designs (see **Section J, Attachment Y** for the Draft ARNG JIE Implementation plan). This planning includes identifying new technologies and technology trends that may positively impact its capability to deliver quality services. The contractor shall forecast service demand and assess opportunities in

unmet or underprovided customer needs. The contractor shall examine services and processes to assess and review current EOSS needs and utilizations in light of new and emerging technologies.

The contractor shall:

a. Provide the following types of technology planning support:
    1. Continually evaluate the IT marketplace, its trends, and growth.
    2. Maintain list of business requirements and the corresponding Service Pipeline.
    3. Provide input to the ARNG's Strategic Plan.
    4. Develop and enhance demand management processes, ensuring current and proposed services are right-sized to demand or resources.
    5. Use broad current technical and business process knowledge, the contractor shall establish future customer technology and process goals and define current infrastructure and services baseline.
b. Develop Technology Trending Reports (**CDRL 05**) (**Section F, Deliverable 18**) that analyze the industry trends and present the potential impact of these trends on the current and planned ARNG's activities.
c. Evaluate the impact of technology trends on the Integrated Master Schedule (**CDRL 04**).
d. Develop and periodically update the technology refresh portion of the Service Strategy section of the IT Service Management Plan that takes into account current ARNG technology plans and adjust them based on the EOSS expansion plans and developments in the IT industry. The contractor shall provide long-term and short-term technology refresh and modernization strategy updates to the TRP. The contractor shall propose alternative technology refresh strategies to implement proposed initiatives in Service Design.

C.5.4.2.3 SUBTASK 2.3 - FINANCIAL MANAGEMENT/ACTIVITY-BASED COSTING

The contractor shall document baseline TCO and incremental costs for delivering all services provided by EOSS and to reduce TCO utilizing the ITIL mechanism of CSI.

The contractor shall:

a. Develop a means of tracking and presenting individual service costs (TCO and incremental). ARNG requires the contractor to track costs on per activity basis, such as cost per service contact, per project, per service, and end customer (e.g., email, AD).
b. Align the services costs to the most current Army C4IM services list.
c. Develop financial and operational expansion estimates including Return on Investment (ROI) and cost avoidance for supporting additional customer requirements and a rough order of magnitude. An example of such an expansion is ability to offer Service Desk service to a state or external organization.
d. Keep track and report on incremental costs associated with supporting expansion.

e. Provide Business Case Analyses to support the initiation or suspension of service delivery. These analyses will support ARNG-IMN decisions to implement or alter the portfolio of services provided.
f. Provide financial estimates and reports of costs and cost avoidance for initiatives/projects/service design packages/changes under consideration.

C.5.4.3 SUBTASK 3 - SERVICE DESIGN

C.5.4.3.1 SUBTASK 3.1 - PROCESS MANAGEMENT

The role of the Service Design functions is to design new or updates to existing services, processes, and technologies into the ARNG IT enterprise environment in a manner that meets availability, capacity, and performance requirements. The contractor shall be responsible for all processes in Service Design.

C.5.4.3.1.1 SUBTASK 3.1.1 - SERVICE LEVEL MANAGEMENT

The contractor shall:

a. Design new or update existing services with specific service levels and critical success factors (CSFs) defined at project conception and agreed to by IMN and project stakeholders.
b. Develop and maintain Operational Level Agreements (OLAs) (**CDRL 10**) (**Section F, Deliverable 19**) identifying roles, responsibilities, and resources required.
c. Draft new or update existing SLAs for all services.
d. Draft new or update measurements, metrics, and KPIs with an emphasis on availability, reliability, and performance for services in coordination with Service owners and CSI.
e. Report and monitor SLAs, SLOs, metrics, and KPIs in the MPSR.
f. In conjunction with CSI, proactively audit service and process owners for compliance with SLAs and SLOs.
g. Coordinate SLM with CSI activities.

C.5.4.3.1.2 SUBTASK 3.1.2 - SERVICE CATALOG MANAGEMENT

The EOSS Service Catalog Framework (see **Section J, Attachment DD**) provides description and performance information about services provided by the ARNG-IMN. Each entry in the service catalog provides details about scope of the service, its availability and pricing, relation to other services, as well as relationship with other services. Typically a catalog will have two views - a customer-facing view from which business users can browse and select services, and a technical view that documents exactly what is required to deliver each service in the catalog. Services in the catalog will align with the current version of the Army C4IM services list. The ARNG is currently developing processes which will allow users to request certain services without a need to contact the Service Desk.

The contractor shall maintain and update the Service Catalog (**CDRL 11**) with all relevant data to include capabilities for Service Request and Tier 0 capabilities.

C.5.4.3.1.3 SUBTASK 3.1.3 - CAPACITY MANAGEMENT

The contractor shall:

a. Ensure all services (new and existing) meet capacity requirements outlined with the corresponding SLA and underpinning resources that can support the service.
b. Coordinate demand management and its effects on resource capacity.
c. Monitor component performance and provide analysis of proposed changes to current infrastructure/resources.

C.5.4.3.1.4 SUBTASK 3.1.4 - AVAILABILITY MANAGEMENT

The contractor shall:

a. Ensure availability for Mission Assurance Category (MAC) I services of GuardNet as well as other managed services while accounting for service continuity.
b. Design service to meet availability requirements as defined in corresponding SLA.
c. Report service and underpinning resources availability at a minimum at the MPSR.

C.5.4.3.1.5 SUBTASK 3.1.5 - IT SERVICE CONTINUITY MANAGEMENT AND CONTINUITY OF OPERATIONS (COOP)

ARNG hosts its managed services at one or more sites, i.e. RCC-NG, Camp Robinson, California JFHQ, including a primary instance and various alternative sites (physical or virtual). The Alternate Site(s) shall have host copies of all tools and management systems used at the RCC-NG or other primary service delivery site. Managed remotely, these systems shall maintain the same configuration as the primary. The contractor shall maintain recovery times IAW SLAs, SLOs, other service availability standards (see **Section J, Attachment Z** for SLAs) and the COOP/Disaster Recovery (DR) Plan consistent for a MAC I system.

The contractor shall:

a. Design, maintain, update, and enhance the EOSS DR/COOP capability to maintain the same level of operational support and ensure that the alternative capability be ready within one hour of the service's failure or designated downtime.
b. Ensure that the alternate systems are:
    1. Maintained with the same software release levels and patches as the primary systems.
    2. Configured with the same configuration information as the primary systems.
    3. Capable of operating on their own in case of partial or full failure of the primary systems.
c. Support the COOP exercises with the following elements:

1. Maintain operational support by using tools and systems available from the alternate RCC-NG or other alternative sites and contractor's facilities and/or resources.
2. Provide support activities using the alternate facilities for the duration of the outage/exercise.
3. Transition operations back to the RCC-NG facility.
4. Update primary operational and support tools and systems (at the primary RCC-NG) with data collected and updated during the outage.
5. Initiate operations from the primary RCC-NG.
6. Re-synch primary and alternate systems.
7. Stand down the alternate operations.

d. Maintain and operate alternative sites' tools service the same as the primary site as a result of new or changed services, support directives, or security mandates.
e. Develop, maintain, test, and implement back-up and restore SOPs and maintain off-site backups.
f. Develop, test, and maintain a Disaster Recovery Plan (**CDRL 12)** (**Section F, Deliverable 20**) IAW RCC-NG COOP.
g. The contractor shall develop, maintain, test, and execute a COOP during emergency or training situations.
h. Provide an After Action Report (AAR) (**CDRL 05**) (**Section F, Deliverable 21**) in the event of an outage, disaster, or exercise
i. Ensure that service owners have planned and documented the necessary alternative site resource requirements and that these are periodically reviewed and tested.

C.5.4.3.1.6 SUBTASK 3.1.6 - SUPPLIER MANAGEMENT

In providing enterprise-wide IT services, the ARNG G6 organization acts as the de facto integrator for delivery of enterprise IT services to the ARNG. ARNG employs services of multiple contractors and Government agencies that provide the different services needed to support the infrastructure as well as to manage and implement the network. The ARNG G6 establishes contractual SLAs for each underpinning supplier contracts to ensure performance targets are met. Figure 2 is a high level illustration of how these relationships support Enterprise operations.

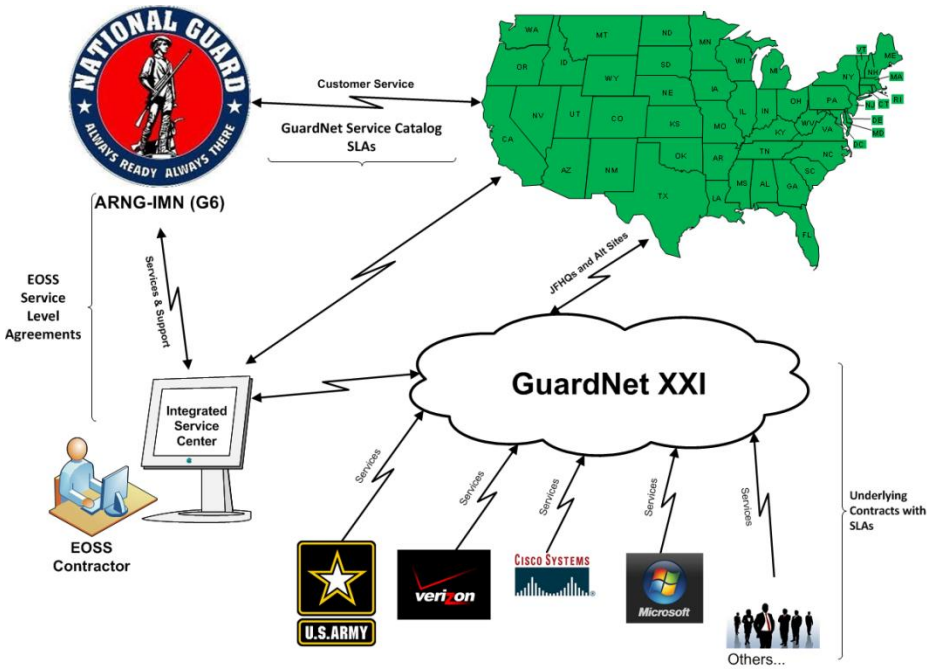

Figure 2 GuardNet and EOSS Supplier Relationships

The EOSS contractor is expected to work cooperatively with other contractors and vendors in executing the requirements of the EOSS TO. See **Section J, Attachment BB** for a list of these contractors.

The contractor shall establish working agreements that enable it to meet the ARNG-dictated performance agreements under the EOSS TO in accordance the Program Management Plan (**CDRL 01**). Examples of such coordination may include:

a. Establish memoranda of understanding (MOUs) with other suppliers as needed to perform required functions.
b. Establish incident and problem resolution escalation paths between the EOSS Service Desk and other organizations within the ARNG.
c. Troubleshoot guides that enable the EOSS Service Desk to limit the number of escalated issues.
d. Provide Service Desk scripts that support a common approach to issues classification, description, routing, and resolution.

The contractor shall manage GFE warranty and maintenance agreements which are further defined in **Section C.5.5.5.1**. Government service providers/regulatory authorities/peers/partners include DISA, Army's 2nd Regional Cyber Center (RCC), Network Command (NETCOM), U.S. Army Cyber Command (ARCYBER), Federal Bureau of Investigations (FBI), and Department of Homeland Security (DHS).

C.5.4.3.1.7 SUBTASK 3.1.7 CYBER/INFORMATION SECURITY

The contractor will be responsible for ensuring the following aspects of Cyber Security: physical, personnel, facility, information systems, and through policies and controls IAW AR25-2, DHS Interagency Security Committee Standards (DHS ISC), and DoD 5220.22M, 8500.2, 8570.01-M. The contractor shall manage information security risks and report findings to the Government. Cyber Security tasks are further defined in **Sections C.5.5.3.13.1-5.**

C.5.4.3.2 SUBTASK 3.2 - PROJECT DESIGN AND COORDINATION

The contractor shall:

a. Support individual IT initiatives and projects that may address all aspects of ARNG Enterprise and business operations for the purpose of improving and expanding the ARNG Enterprise service offerings. These projects will be performed as part of ongoing Operations and Maintenance (O&M) requirements or as Government-Directed Initiatives (GDI) as described below. These projects will be managed as separately defined and self-contained work efforts that have an approved schedule, specific requirements, and defined critical success factors.
b. Improve upon and manage the process by which all project initiatives are collected, managed, reviewed, and approved before resources are allocated for them. These initiatives may be externally or internally generated requirements.
c. Implement and continually improve Agile project management methodology and incorporate Agile methodology into the existing EOSS ITIL service management framework.
d. Coordinate and convene initiative review panels comprised of the various stakeholders. This initiative review panel will either approve or disapprove initiatives. Once approved, these initiatives become projects/design packages/changes under this EOSS TO.
e. All initiatives/projects/design packages shall conform to appropriate viewpoints IAW the latest DoD Architecture Framework (DoDAF) guidelines and the contractor will update any in-flight projects if needed.

If an initiative requires extensive resources (typically more than 40 hours of work) it requires a Project Implementation Plan as part of the design package. The costs of preparing the design packages shall be included in the EOSS operations and maintenance activities.

C.5.4.3.2.1 SUBTASK 3.2.1 – CHANGE/INITIATIVE/PROJECT/SERVICE DESIGN PACKAGES

The contractor shall:

a. Develop Service Design Packages (**CDRL 13**) (**Section F, Deliverable 22**) that contain the following at a minimum:
    1. Systems Documentation
    2. Test Plan

3. Test Procedures
4. Draft Test Summary
5. System Architecture diagrams/schemas IAW DoDAF
6. Bill of Materials
7. Draft Training Documentation
8. Service Catalog Description
9. Business Case Analysis/Analysis of Alternatives including five-year operations and maintenance estimate
10. IMS Effect
11. Project Implementation Plan
12. Proposed Policies and Procedures
13. System Integration Plan
14. Other artifacts dependent upon process improvements/refinements implemented by the contractor
15. Effects on configuration items (CIs)

b. Provide weekly project updates in the TSR.
c. Document and track directives and mandates that impact GuardNet services. Frequently these mandates (primarily Army and ARCYBER Chief Technology Office (CTOs)) relate to ARNG initiatives that may trigger changes to services. The contractor shall manage the development and execution as aligned with EOSS initiatives, and tracking of internal CTOs to EOSS customers that outline timelines, impacts, customer dependencies, and objectives in coordination with Service Operations. These changes/initiatives shall follow the same process.

C.5.4.4 SUBTASK 4 - SERVICE TRANSITION

ITIL-based Service Transition supports the planning and execution of delivery activities to transition services from the design stage to the operational environment.

C.5.4.4.1 SUBTASK 4.1 - PROCESS MANAGEMENT

The contractor shall be responsible for all processes in Service Transition.

C.5.4.4.1.1 SUBTASK 4.1.1 - ASSET AND CONFIGURATION MANAGEMENT

The contractor shall:

a. Implement and maintain processes for the management of assets/configuration items.
b. Manage all GFE from procurement to disposal. GFE is further detailed in the Task 5 Managed Service of the TOR.
c. Manage, maintain, update, and enhance the Configuration Management System (CMS) (**CDRL 14**) using ARNG's BMC ITSM 7.6 or higher for all Configuration Items (CIs)

and their relationships to other CIs and artifacts. Process artifacts, such as incident, problem, and change records.

d. Develop and perform Configuration Audits (**CDRL 05**) (**Section F, Deliverable 23**) in coordination with operations to verify the information in the CMS is the same as in production.

C.5.4.4.1.2 SUBTASK 4.1.2 - KNOWLEDGE MANAGEMENT

The contractor shall:

a. Update and maintain BMC ITSM Knowledge Module and Documentation Library.
b. Maintain SOPs and job aids ensuring they are current and easily accessed.
c. Assist service and process owners with development of training for new or changed services/processes.
d. Track usage of knowledge and develop processes to improve knowledge transfer and training.

C.5.4.4.2 SUBTASK 4.2 – TRANSITION MANAGEMENT OF PROJECTS/CHANGES

The contractor shall be responsible for the transition of Service Design Packages/projects/changes into a Request for Change (RFC) that is submitted to the Change Advisory Board (CAB) for approval before proposed changes to the production environment are enacted and will become a Release Package. These SDPs/projects/changes shall be constantly updated on the Integrated Master Schedule in coordination with Service Design.

The contractor shall develop RFCs that will contain, at a minimum, the following:

a. Systems Documentation
b. Test Plan
c. Test Procedures
d. Draft Test Summary
e. System Architecture Diagrams/Schemas IAW DoDAF
f. Bill of Materials
g. Draft Training Documentation
h. Service Catalog Description
i. Release Policy Plan and Documentation
j. Integrated Master Schedule Effect
k. Project Implementation Plan
l. Proposed Policies and Procedures
m. System Integration Plan
n. CI affects
o. Impact and risk assessments

p. Success Criteria
q. Relationship to other services & processes
r. Change procedures
s. Rollback procedures
t. Draft Network Maintenance Alert
u. Other artifacts dependent upon process improvements/refinements implemented by the contractor

C.5.4.4.2.1 SUBTASK 4.2.1 - CHANGE MANAGEMENT

The contractor shall:

a. Manage all changes to GuardNet services and infrastructure ensuring the lowest level of risk.
b. Prioritize and review all RFCs.
c. Evaluate all changes
d. Schedule and coordinate Government-run review boards such as CAB and Post-Implementation Review to authorize all changes.
e. Ensure all changes are recorded in the CMS.
f. Support service validation and testing and release and deployment as necessary.
g. Provide reports on change activity in the MPSR.

C.5.4.4.2.2 SUBTASK 4.2.2 – SERVICE VALIDATION AND TESTING

The Enterprise Lab, co-located with the RCC-NG and SPPN, supports development and testing activities and is maintained separately from the production systems. The lab provides a safe environment to perform tests and analyses on new tools, equipment, and software to discover design flaws, inefficiencies, performance issues, or incompatibilities prior to fielding them live on the network. There will be a single test lab in the SPPN. The contractor shall test all changes before release in the live environment.

The contractor shall:

a. Establish and maintain an enterprise development, integration, test, and validation environment that emulates the production environment. Due to its prohibitive costs, the lab does not contain copies of all the operational systems, but is configured to test updates and changes to a majority of them.
b. Provide separate ‘development’ and ‘test’ resources with management controls to ensure adequate integrity of the development and testing processes.
c. Use this Enterprise Lab to test enhancements/new configurations of the current operational systems and/or test replacement equipment and systems.
d. Place emphasis on pre-deployment testing of new tools, updates, and patches, including rollback procedures and simulation.

e. Provide test results to change management.

C.5.4.4.2.3 SUBTASK 4.2.3 - RELEASE AND DEPLOYMENT MANAGEMENT

The contractor shall be responsible for all release and deployment processes and release planning of changes to the live environment. The contractor shall transition SDPs/changes/projects to Service/Release Packages (SRPs) for new, changed or retired services upon approval from the CAB. The SRP shall include:

a. Release technical description.
b. Release site(s) location(s).
c. Release Plan of Action and Milestones (POA&M).
d. Site and location of facility requirements (e.g., power, Heating, Ventilation, and Air Conditioning (HVAC)).
e. Site physical security requirements.
f. Site environment and safety considerations.
g. Release build and test operational and verification plan.
h. Plan for user and organization communications (as required).
i. Plan to update all affected documentation including site drawing packages; integrated architecture, engineering, and operations supporting documentation; asset data; and CIs in the CMS.
j. Identified risks and mitigation strategies.

The contractor shall provide early life support for deployed changes. The contractor shall conduct post-implementation reviews and coordinate the closure of the ticket with change management.

C.5.4.5 SUBTASK 5 - SERVICE OPERATIONS

The contractor shall operate, manage, and secure equipment and systems used by the EOSS program to deliver services identified in the Service Catalog and to deliver these services to the ARNG users. The contractor shall be responsible for all processes in Service Operations.

C.5.4.5.1 SUBTASK 5.1 - EVENT MANAGEMENT

The contractor shall respond to service operational events, e.g. system-related outages and security situations.

The contractor shall:

a. Provide event management.
b. Provide real-time situational awareness of events and report those to the Government.
c. Respond to events.

d. Report any events in the MPSR to include:

1. Total number of events for the reporting period.
2. Summary and analysis of the event triggers that resulted in incidents for the current reporting period.
3. Problems nominated as a result of events.

C.5.4.5.2 SUBTASK 5.2 - INCIDENT MANAGEMENT

The contractor shall:

a. Provide incident management.
b. Log, categorize, prioritize, allocate, track, and escalate incidents.
c. Provide the status and summary of incidents in the MPSR.
d. Respond to incidents and notify the Government as necessary such as in the case of escalation.
e. Use BMC ITSM as the incident repository.
f. Incident analysis is further detailed in **C.5.5.4.3.**
g. Ensure that the notification about unscheduled maintenance is posted IAW SLAs.
h. Communicate scheduled maintenance notification IAW SLAs.
i. Communicate information about known issues/outages and their anticipated resolution times as described in the SLAs.

C.5.4.5.3 SUBTASK 5.3 - PROBLEM MANAGEMENT

The contractor shall:

a. Implement, maintain, and enhance Problem Management processes and activities.
b. Identify, monitor, diagnose, mitigate, and report problems.
    1. Perform pro-active problem management on event and incident data.
    2. Perform reactive problem management on availability, capacity and demand, event, incident, and Government-provided data.
    3. Establish and track problem records in the Problem Management tracking tool to relate incident or event data and document problem artifacts.
    4. Identify underlying root cause of assigned problems.
    5. Develop workarounds and create known error records in a Known Error Database, if applicable. Include the following information within the error records:
        A. Clear, concise problem statement.
        B. Determination for root cause investigation.
        C. Process (incident, event, or Government) from which the problem originated.
        D. Significance of the problem and related effects.

E. Extent of the problem.
F. Timeframe of the problem, where possible.
G. Detailed explanation of problem solutions.

6. Find or create a problem solution.
7. Determine resolution and assist in planning and generating RFC(s), as required, to resolve problem.
8. Recommend to the Government convening joint service provider resolution sessions to resolve problems.

c. Implement approved problem solutions.
d. Problem and root cause analysis is further detailed in **Section C.5.5.4.3.**

C.5.4.5.4 SUBTASK 5.4 REQUEST MANAGEMENT

The contractor shall:

a. Manage the life cycle of all service requests from users.
b. Improve service request processes.
c. Provide innovative solutions to manage user service requests.

C.5.4.5.5 SUBTASK 5.5 - ACCESS MANAGEMENT

The contractor shall:

a. Implement, maintain, and enhance Access Management processes and activities.
b. Validate access requests for services.
c. Maintain systems or interfaces that provide validation/verification of user credentials.
d. Monitor, log, track, and manage access activities and notify the Government of violations and remove or restrict access.

C.5.5 TASK 5 - MANAGED SERVICES

C.5.5.1 SUBTASK 1 ENGINEERING AND PROJECT SUPPORT

The contractor shall establish a GuardNet Engineering group that supports the Service Delivery process by providing enhanced technical knowledge and analysis to the operation and maintenance activities. In addition, the GuardNet Engineering team members provide configuration management as well as planning required to meet availability and capacity requirements of the current EOSS services now and in the future.

The contractor shall:

a. Provide O&M engineering support for, but not limited to, the following:

1. Network Architecture Planning and Management, Integration and Implementation, and Network Performance Analysis.
2. Security Architecture Planning, Integration and Implementation, and Performance Analysis.
3. Information Assurance.
4. Department of Defense Risk Management Framework (RMF).
5. Enterprise Application Design and Impact Analysis.
6. Enterprise Management Tool Analysis and Development.
7. Technical Project Management.
8. Video and Audio Teleconferencing.
9. Telephony.
10. Net worthiness.
11. Computer network defense.
12. Service Desk.
13. Hand-held Devices.

b. Provide engineering support for all changes to the ARNG IT Enterprise infrastructure and its service offerings. This support includes technical activities as well as establishing priorities, adjusting schedules, projecting staffing, estimating rough costs, and developing high-level Concept of Operations (CONOPS) documentation. Projects may encompass all facets of the enterprise operations (e.g., voice, video, data, system, and network design/redesign).
c. Provide Tier II and III support to the Service Desk in problem and incident resolution.
d. Develop TCO projections.
e. Develop project initiatives/service design packages/changes/projects requested by the ARNG.

C.5.5.2 SUBTASK 2 - DATA NETWORKS SYSTEM ENGINEERING

Data network engineering includes processes associated with designing and implementing changes to the GuardNet network.

The contractor shall:

a. Provide telecommunications engineering support to the ARNG to maintain the support of the enterprise network and processing nodes and infrastructures.
b. Provide engineering services to monitor, design, and evaluate these networks and processing nodes and infrastructures to include examining sizing, perform network modeling, mapping, and provide projected costing.
c. Ensure that capacity management such as bandwidth and throughput requirements are considered during any design/redesign effort.

C.5.5.2.1 SUBTASK 2.1 - IP MANAGEMENT

The contractor shall:

a. Maintain and manage Internet Protocol (IP) address range configurations IAW availability and capacity service level agreements for GuardNet including recommendations for improvement.
b. Ensure the bandwidth and telecom service requests are accomplished for the RCC-NG Local Area Network (LAN) and GuardNet WAN routing design (see **Section J, Attachment U**) based on the SLAs contained in **Section J, Attachment Z**.
c. Maximize IP ranges for desired performance of all GuardNet services.
d. Balances GuardNet and SIPRNet traffic across the logical boundary.

C.5.5.2.2 SUBTASK 2.2 - BANDWIDTH MANAGEMENT

The contractor shall:

a. Monitor, gather, and aggregate utilization data.
b. Analyze usage with availability and capacity SLAs as well as future capacity requirements.
c. Identify problems and provide recommendations and solutions for corrective action.
d. Implement approved corrective actions.
e. Report bandwidth management activities in the MPSR.

C.5.5.2.3 SUBTASK 2.3 – NETWORK TELECOM SERVICE REQUESTS

The contractor shall:

a. Initiate telecom service requests (TSRs) (connect, disconnect, and modify).
b. Track progress and status of orders in a central database.
c. Manage circuit and service inventory including address and configuration information.
d. Collaborate and coordinate with the MPLS vendor.
e. Manage telecom invoices (GuardNet, DISA, DLP, and Networx service) on behalf of the ARNG, verifying service IAW the applicable contract, and managing credits for outages:
    1. Review invoices for accuracy based on contract-specific rates and circuit identifications (IDs).
    2. Correlate circuit outage information with the credits appearing in the invoices IAW the underpinning contracts.
    3. Coordinate payment and credit issue resolution with the service providers.
    4. Forecast circuit budgetary requirements.
    5. Track payment status.
    6. Maintain historical payment data information.

f. Report discrepancies between expected expense and invoiced expense as well as recommendations for correcting inaccuracies and credits to the Government.

C.5.5.3 SUBTASK 3 – ENTERPRISE IT SERVICES & SUPPORT

The contractor shall provide Service Operations support for the tasks and activities that are needed to successfully maintain ARNG's enterprise computing infrastructure and provide end-user support.

ARNG has established SOPs for the operations and maintenance of the EOSS program.

The contractor shall:

a. Establish and maintain formalized Standard Operating Procedures (SOPs) and operational plans for each functional labor category.
b. Deliver these (new or updated) SOPs for review and approval by the Government as outlined in the PMP.
c. Ensure the availability and accessibility of SOPs.
d. Monitor usage through knowledge management processes.

C.5.5.3.1 SUBTASK 3.1 - BMC® ITSM SYSTEM SUPPORT

The ARNG uses the ITSM system and its various modules to manage and report on the incident, problem and request resolution processes and to manage approval process for various projects. The criticality of this tool set requires dedicated maintenance efforts. The contractor shall be responsible for maintenance of all Remedy and Kinetic modules, as well as integration of these with external systems.

The contractor shall:

a. Maintain and update the ITSM system into the operational environment and provide ongoing operational support of the ARNG's ITSM v.7.6, or higher system modules.
b. Provide the following support:
    1. Introduce changes and enhancements into the ITSM operational environment.
    2. Develop Service Desk SOPs based on the new functionality.
    3. Maintain operational readiness of the BMC ITSM system modules, third-party modules, and the associated Structured Query Language (SQL) databases (primary and backup) IAW SLAs.
    4. Manage appropriate numbers and types of user licenses.
    5. Implement workflow changes as required by changing environment.
    6. Update data selection.
    7. Build automated reports.
    8. Maintain user accounts.

9. Perform standard administrative system configuration (such as add location, groups, etc.).
10. Maintain the SQL databases supporting the ITSM implementation.
11. On-board customers using standard ITSM module configurations.

C.5.5.3.2 SUBTASK 3.2 - ENTERPRISE SERVICE DESK (ESD)

The Enterprise Service Desk (ESD), provided by the contractor, is the end-user Point of Contact (POC) for all service support and is a critical element of the customer's perception of how well the ARNG G6 performs its mission. The ESD handles incidents and requests and provides an interface for activities such as changes, problems, configuration, releases, service levels, and IT Service Continuity Management. All incidents are managed using the Government's incident handling system.

ESD is organized into support tiers: Tier 0 (self-service) provides service applications, Tier 1 provides immediate end-user interface (e.g., phone, Web mail), Tier 2 provides system administrative support, and Tier 3 provides engineering-level troubleshooting and configuration changes through the GuardNet Engineering Team, occasionally with assistance from the vendors. The EOSS contractor shall perform at all tiers. Tiers 0 and 1 support are described in the subsections below. The contractor shall provide Tiers II and III support for the operations processes listed here in support of Task 5 Subtasks one through five:

a. Event Management
b. Incident Management
c. Problem Management
d. Request Management
e. Access Management

ESD also provides different support levels based on agreements with the states, territories, and Washington, D.C.

See current ARNG State Service Levels in **Section J, Attachment FF**.

The priorities of the EOSS ESD are:

a. To manage the problem management, incident management, and request fulfillment processes.
b. To manage customer service expectations by identifying and communicating services to customers.
c. To return the customer to normal operations within SLA requirements and specifications.
d. To continually improve service performance.
e. To perform consistent workflow support enabling service request escalations across disparate IT infrastructure contracts.
f. To provide updates about outages and problem resolution efforts.

g. To collect, consolidate, analyze, and report performance metrics for services provided to customers.
h. To provide the ARNG G6 with accurate and appropriate data that enables responsible operational decisions.

The contractor shall:

Provide Service Operations support on 24x7x365 basis in a manner that meets or exceeds the applicable SLAs. See **Section J, Attachment GG** for historical service statistics and metrics.

C.5.5.3.2.1 SUBTASK 3.2.1 - TIER 0 SPECIFIC TASKS

The contractor shall:

a. Configure and integrate with the ARNG's ITSM system Kinetics modules, which provide self-service functionality, such as finding answers, ordering a service or product, checking the status of a ticket, subscribing to and viewing notifications regarding services outages, and creating tickets.
b. Report on utilization and make improvement recommendations.

C.5.5.3.2.2 SUBTASK 3.2.2 - TIER 1 SPECIFIC TASKS

The ESD is the first point of contact for end-users seeking assistance. All requests for service are routed to ESD via a toll-free telephone access method, email, or the Web.

The contractor shall:

a. Provide Tier 1 support for the following support functions to end-users who use EOSS-managed or controlled systems and/or equipment:
    1. End-user support:
        A. Assist with application usage questions.
        B. Coordinate requests for a new system or upgrades to the existing system (software and hardware).
        C. Coordinate requests for new telecommunication services.
        D. Coordinate requests for asset and staff moves. (The move is performed by local staff.)
    2. Resolve domain issues:
        A. Password resets.
        B. End-user account creation/deletion.
        C. Profiles, including access permissions and end-user profiles.
    3. LAN support:
        A. Verify connectivity.
        B. Assist with proper workstation LAN configuration remotely.

C. Monitor network alerts.

4. WAN support:
   A. Verify connectivity.
   B. Monitor network alerts.
5. Assist with usage of the video and audio equipment remotely.
6. Not reject a caller based upon a problem not being within their purview. The contractor shall make every effort to initially solve the problem or refer it to the most appropriate support organization or Tier-level support.
7. Use the ARNG-owned ITSM system for handling all incident/request/problem (trouble) tickets.
8. Escalate tickets to Tier II/III as necessary.
9. Report Tier 1 metrics.

C.5.5.3.2.3 SUBTASK 3.2.3 - HANDLING USER CONTACT

As stated above, all requests for service from the end users are routed to the ESD for initial handling.

The contractor shall:

a. Provide live coverage 24x7x365 at the RCC-NG.
b. Answer calls in a manner required by applicable SLAs.
c. Greet the customer with a standard (ARNG-dictated) welcome message.
d. Verify existing or obtain new end-user information, such as locations, organizations, and contact information.
e. Identify the nature of the problem and classify it correctly.
f. Record any additional information obtained from the end user.
g. Assign priority.
h. Provide the end user with a ticket number.
i. Escalate the tickets, as required, by assignment to the appropriate group or Tier Level.

C.5.5.3.2.4 SUBTASK 3.2.4 - TICKET UPDATES

The contractor shall:

a. Properly manage tickets created by or assigned to the contractor using the following criteria:
   1. Update all tickets as required by the SLAs.
   2. Maintain status of all open trouble tickets and escalate as required.
   3. Coordinate resolution with other internal and external teams, as appropriate.

4. Update the end users with progress of the incident resolution through the trouble ticket updates.
5. Check the assigned tickets queue on regular basis throughout the support hours.
6. Check for requests coming through the website, email, and fax on regular basis and create trouble tickets based on these requests as required by the appropriate SLAs.
7. Provide advice and guidance to the end users regarding restoration of interrupted service.

b. Own the problem resolution process from the initial contact with the end users to resolution of the incident regardless of whether the problem is resolved by Tier II/III or it has to be escalated to other organizations.
c. Ensure that the end users are updated with the progress of the resolution process; the contractor's staff shall provide updates to the end users on a regular basis as defined by the SLAs.
d. Be responsible for verifying resolutions with the end users, by doing regular checks with ticket submitters of a subset of resolved tickets, to verify end-user concurrence in the resolution.

C.5.5.3.3 SUBTASK 3.3 - INCIDENT ANALYSIS

The incident resolution process involves both immediate assistance to the end users and analysis of the encountered issues. To increase efficiency of employed systems and to minimize disruption to the ongoing operations, the Government expects incident analysis to decrease response times, maintain user satisfaction, quickly restore normal operations, and reduce the occurrence of incidents in the future.

The contractor shall:

a. Provide initial diagnosis, when possible leveraging Knowledge Management.
b. Constantly monitor event and incident tickets to proactively identify, in real time, incident trends.
c. Provide recommendations that are not limited to technical solutions only, but shall also incorporate suggestions for improving internal processes, as appropriate.
d. Open problem tickets for incidents depending on the nature and/or frequency of the incident/incidents.
e. Present the summary results of incident analysis, along with recommendations for improvement, on a regular basis as part of the standard MPSR.

C.5.5.3.4 SUBTASK 3.4 - PROBLEM ANALYSIS

The identification of root cause of problems as defined in ITIL and the means of resolving them is not limited to technical solutions only, but can also incorporate suggestions for improving internal processes, as appropriate. Continual analysis with summary recommendations for improvement will allow the Service Desk to proactively anticipate and resolve potential end user problems.

The contractor shall:

a. Support Problem Management processes/activities.
b. Conduct problem analysis on all problem tickets.
c. Perform root cause analysis using approaches, such as Kepner and Tregoe, using appropriate analysis techniques to identify the underlying cause of the problem, its overall impact, and solutions for eliminating this cause in the future.
d. Ensure that every problem ticket is updated with information about the root cause of the problem.
e. Update the Known Error Database (KEDB) with known errors, work a rounds, and solutions.
f. Test and vet proposed solution through the change management process before releasing into production.
g. Support problem analysis of known errors detected during development and ensure those that are released into production are logged in the KEDB.

C.5.5.3.5 SUBTASK 3.5 – GUARDNET HOSTING INFRASTRUCTURE AND TOOLS SUPPORT

Tools are used to support GuardNet Managed Services as well as IT Service Management by providing enhanced capabilities to monitor, manage, and protect GuardNet. Examples of the EOSS tools categories are network management, monitoring, access management, IT service delivery, incident management, cyber security tools, patch management, and configuration management. GuardNet hosting infrastructure includes servers, databases, and software to run and manage GuardNet services such as Active Directory and OCSP as well as tools.

The contractor shall:

a. Ensure all tools and corresponding infrastructure are properly maintained, configured, and patched IAW SLAs, regulations, STIGs, CTOs, ARs and best business practices in both physical and virtual environments and that all changes to these environments follow established IT Service Management processes.
b. Provide patch management support including:
    1. Test all security patches provided by the industry and the DoD to ensure they do not have negative impact on the operational systems, using the lab environment when applicable.

2. Review waiver requests and present recommended actions to the ARNG.
3. Maintain a record of one and two above for all patch testing and patched systems.
4. Develop software packages/updates via System Center Configuration Manager (SCCM) or other distribution method such as a Definitive Media Library to deploy/deliver or make available patches and updates IAW the System Management System (SYSMAN) initiative.
5. Provide Tier II/III support to ARNG states, territories, and Washington, D.C. to support their efforts in patch management, ranging from break fix to preparing for inspections.

c. Provide performance monitoring and management of Cyber Security measures including providing security services for protection of the network.
d. Provide Enterprise Tier II and III support for tools and equipment under contractor management.
e. Support Continual Service Improvement, Service Design, and Service Transition activities as necessary.
f. Maintain, enhance, and maximize the capacity and deployed capabilities of tools and infrastructure under management and consult on enhancements and /or modernization of supporting hardware and software.
g. Provide Enterprise replication, back-up, and restore for GuardNet services and systems assuring service availability and IAW service SLAs, and COOP/Disaster Recovery plan. Periodically test this functionality providing validation of capability and processes.
h. Leverage remote access services to provide operational capabilities at alternate sites IAW COOP.
i. Provide hosting, tool, and infrastructure metrics.

C.5.5.3.6 SUBTASK 3.6 – GUARDNET/GUARDNET-S OPERATIONS AND MAINTENANCE

Operations and maintenance activities are required to properly manage and configure the ARNG-owned GuardNet/GuardNet-S edge devices. As explained earlier, the ARNG WAN provider provides connectivity between ARNG sites, terminating traffic at their site routers. ARNG is responsible for accepting this traffic and routing it further within the state-level enclave.

The contractor shall:

a. Maintain the operational capability of the GuardNet/GuardNet-S WANs IAW the applicable SLAs.
b. Support operations of the GuardNet/GuardNet-S WAN through the following tasks:
   1. Monitor all network management systems and respond to all network alerts in a manner required by the applicable SLAs.
   2. Isolate and resolve network faults.
   3. Maintain, upgrade, and troubleshoot all GuardNet network elements:
      A. Routers.

B. Hubs.
C. Switches.
D. Firewalls.
E. Domain Controllers to include NG, National Guard Application System (NGAPPS), and DLP domain.
F. Top Level Architecture (TLA) stacks.
G. Security devices.
H. Classroom routers and switches.
I. Enterprise audio and video conferencing equipment, to include MCUs and bridges.

4. Configure and update router modules.
5. Maintain access to the NIPRNet.
6. Maintain data transport from the GuardNet to other DoD networks via SIPRNet as appropriate. Currently, there is a single SIPRNet connection at the EOSS TO's RCC-NG facility; however, the RCC-NG will manage the GuardNet-S WAN once it is fully implemented.
7. Provide a local presence on SIPRNet for access by appropriately cleared contract and Government staff. Report classified spillage.
8. Maintain trust relations and interconnectivity with the states, other DoD agencies, and others as required.
9. Coordinate with the network telecommunications service providers in resolving service problems.
10. Monitor and manage network telecom service providers SLAs and work with the providers to resolve issues.
11. Coordinate with the National Capital Region (NCR) staff (Director of Information Management (DOIM), J6, G6) in resolving data communication problems.
12. Monitor circuit utilization and (upon approval) manage bandwidth upgrades/reduction as required.
13. Develop and maintain site-specific equipment inventory and configuration. The site-specific information shall include Enterprise-level elements as well as:
    A. As-built diagrams and schematics.
    B. Rack space layouts.
    C. Equipment interconnectivity.
14. Develop and operate comprehensive network monitoring and management systems.
15. Troubleshoot connectivity and configuration issues.
16. Conduct direct support of video and audio conference rooms (at the contractor-provided facility), including remote assistance with operation and maintenance of the Audio/Video (AV) equipment.
17. Support asset management and configuration management activities.
18. Support Service Design and Service Transition activities/processes as necessary.
19. Provide Tier II/III assistance to the states as requested by the ARNG.

C.5.5.3.7 SUBTASK 3.7 - SERVICE SATISFACTION SURVEYS

The ARNG measures end-user and customer satisfaction with contractor's performance via two surveys.

a. Immediate End-User Satisfaction Survey. This survey is automatically initiated upon closure of the incident/problem/requests ticket.
b. Project Leader Survey. The ARNG may send out this survey to the Government staff members who have direct working relationship with the contractor.
c. Provide a survey summary at MPSR.

The contractor shall be responsible for initiating the automated surveys as well as for compiling results and presenting summaries to the Government.

C.5.5.3.8 SUBTASK 3.8 - VIDEO OPERATIONS CENTER (VOC) SUPPORT

The ARNG uses audio/video services extensively to provide communications with the Guard troops stationed throughout the world.

The contractor shall:

a. Maintain enterprise Video Bridging and MCU equipment for audio/video services hosted at two Enterprise locations.
b. Coordinate national and regional audio/video conferences.
c. Support daily audio/video operations.
d. Manage capacity.
e. Troubleshoot connectivity and configuration issues.
f. Conduct direct support of audio/video conference rooms (at the RCC-NG) including remote assistance with operation and maintenance of the AV equipment.
g. Maintain site-specific equipment inventory and configuration.
h. Provide a summary of VOC activities in the MPSR.

C.5.5.3.9 SUBTASK 3.9 – REMOTE CLASSROOM SUPPORT

ARNG uses its video classrooms to provide efficient and effective means of educating its staff. Currently, there are approximately 400 classrooms located at ARNG facilities throughout the United States. Each classroom can accommodate between 5 and 15 student and includes workstations, a central server, and standardized video equipment, including:

a. Tandberg codec.
b. Creston controller.
c. Classroom hub(s) and router(s).
d. Video projectors and audio equipment.

e. Other video-specific equipment.

The classrooms use the GuardNet WAN to access centralized resources. The connectivity is provided via the local/base LAN/MAN, or via dedicated circuits that extend from the GuardNet WAN termination locations (JFHQs).

The contractor shall remotely:

a. Assist with maintenance of the classroom servers and workstations (service and security patches, software distribution, etc.).
b. Troubleshoot audio and video equipment and connectivity.
c. Assist with establishing and troubleshooting video and audio connections.
d. Monitor, manage, and maintain classroom router and switch equipment.
e. Monitor, manage, and maintain DLP network Domain Controllers.
f. Provide support to the states and territories with monitoring and managing classroom dedicated T1 circuits.

C.5.5.3.10 SUBTASK 3.10 - ACTIVE DIRECTORY (AD)

AD is used to authenticate and authorize all users and computers in a Windows domain type network by assigning and enforcing security policies for all computers and installing or updating software.

The contractor shall:

a. Plan, deploy, and operate the ARNG AD domain structure.
b. Support the following requirements:
    1. Manage all objects within the AD structure.
    2. Maintain ARNG AD forest root and Administrative Domains along with state-level AD structures, as required.
    3. Manage access control to the Enterprise Administrators group.
    4. Maintain and update:
        A. Domain plan and design documentation.
        B. Organization Unit (OU) plan.
        C. Enterprise Group Policy.
        D. Trust relations with external AD structures.
    5. Assist states and territories in AD deployment and management activities.
    6. Manage site replication.
    7. Manage security patches and antivirus signatures on ARNG domain controllers.
    8. Perform troubleshooting of the DNS.
c. Maintain and update:
    1. Domain plan and design documentation.

2. Organization Unit (OU) plan.
3. Enterprise Group Policy.
4. Trust relations with external AD structures.
5. Assist states and territories in AD deployment and management activities.
6. Manage site replication.
7. Manage security patches and antivirus signatures on ARNG domain controllers.
8. Perform troubleshooting of the DNS.

d. Assume operational responsibility for additional AD structures as necessary.
e. Report AD activities in the MPSR.

C.5.5.3.11 SUBTASK 3.11 - LOCAL AREA NETWORK (LAN) EQUIPMENT AND SERVICE SUPPORT

The contractor shall:

a. Be responsible for operating, configuring, and managing ARNG's RCC-NG LAN equipment and services (both Contractor-Furnished Equipment (CFE) and GFE).
b. Support the following management systems and services:
   1. Local and privileged-level user account creation and maintenance.
   2. Workstation hardware and software support.
   3. Shared drive and file server support.
   4. Print server, printer, and scanner support.
   5. Provide staff information to validate CAC and account permissions support as requested.
   6. Upgrade and modernize (refresh) equipment and software to meet the needs of the RCC-NG and ensure compatibility with DoD standards. All equipment shall be Energy Star Compliant IAW Far Clause 52.223-15 as contained in **Section I** of the TOR.
   7. Maintain current anti-virus definition files on all equipment.
   8. Deploy emergency patches and other upgrades to equipment provided by the Government.
   9. Maintain connectivity to the GuardNet network.
   10. Ensure any contractor LAN segment connected to GuardNet is isolated from all other non-RCC-NG segments or networks located in the contractor facility.
   11. Ensure that all equipment is connected to only the Guard network and no other network.
   12. The contractor shall monitor vulnerabilities and apply security patches IAW NSA, DISA, and NETCOM.
   13. DoD Enterprise Email (DoD EE) configuration, support, and escalation.

C.5.5.3.12 SUBTASK 3.12 - ENTERPRISE VIRTUAL PRIVATE NETWORK (EVPN)

The contractor shall support and maintain the Enterprise Virtual Private Network (EVPN) and associated groups/accounts for ARNG. ARNG currently uses a Juniper SSL VPN gateway supporting client access via Juniper clients on an Army Gold Master (AGM) imaged device or a Lightweight Portable Security (LPS) disk. The contractor shall provide support for users and media for contractors and staff that are serviced by the contractor-provided LAN. The contractor shall maintain the compatibility of the LPS with GuardNet infrastructure and systems.

C.5.5.3.13 SUBTASK 3.13 – CYBER SECURITY SUPPORT

The contractor shall maintain the enterprise network in a manner compliant with Federal Information Security Management Act (FISMA), DoD RMF and NIST guidance.

C.5.5.3.13.1 SUBTASK 3.13.1 - SECURITY MANAGEMENT SUPPORT

Security Management supports many of the other areas of GuardNet Managed Services as well as IT Service Management tasks ensuring that security considerations are accounted for or Security Management is a sub-process to other tasks. Security Management follows the most current version of CJCS 6510.1, AR 25-2, AR 380-5, DoD 8500, NIS SP 800-53, NISPOM DoD 5220.22-M, and DoD 8530.

Governance and Compliance

The contractor shall:

a. Ensure that GuardNet and its management systems are in compliance with all Information Assurance Vulnerability Alerts (IAVA).
b. Track IAVA compliance at the Enterprise level as well as state compliance.
c. Create and submit appropriate security-related reports, such as required by IAVA: intrusion, virus infection incidents, FISMA and others as requested by the Government.
d. Create POA&M for identified vulnerabilities.
e. Report ARNG compliance to higher level authorities and/or reporting structures.

Management and Policy

The contractor shall:

a. Maintain the Information Security Plan.
b. Support and validate access requests for GuardNet and Managed services through Service Operations.
c. Provide consultation on Cyber Security perspectives for proposed changes/initiatives/projects in any of the Task 4 areas.
d. Monitor and review development in the technology and regulations governing the industry, DoD, and Federal Government security operations.

e. Provide oversight of Cyber Security for ARNG.
f. Maintain and draft memorandums for record, system interconnection agreement, and/or equivalent to document any and all system connections to GuardNet.
g. Validate EOSS managed assets are in compliance with Army Gold Master configuration, NSA Configuration Guidance and NIST Configuration Guidance through coordination with Asset Management.
h. Provide oversight to ensure that the closed area of the RCC-NG complies with NISPOM and AR 380-5.
i. Provide cyber security/information assurance assistance to ARNG states, territories and DC.

C.5.5.3.13.2 SUBTASK 3.13.2 – CERTIFICATION & ACCREDITATION SUPPORT

The contractor shall:

a. Ensure GuardNet and GuardNet-S maintain the Authority to Connect (ATC) and Authority to Operate (ATO).
b. Maintain and update the GuardNet & GuardNet-S RMF attachments in a manner compliant with Federal Information Security Management Act (FISMA), DoD RMF, and NIST guidance (as detailed specifically in NIST Special Publications (SP) 18, 26, 30, 37, 53, 60 and Federal Information Processing System Publication (FIPS Pub 199) and DoD 8530.1 and/or subsequent manual).
c. Test the security technical controls for the system.
d. Support GuardNet and GuardNet-S C&A, prior to external audit, the contractor shall conduct an internal review and execute all checks and tests as required in DoDI 8500-2 IA Control Checklist for a MAC I Sensitive system.
e. Develop a Security Test and Evaluation (ST&E) Test Plan (**CDRL 15**) (**Section F, Deliverable 25**) that addresses all the requirements identified in NIST SP 800-53 for a High Impact System and the appropriate DoD, Army, and ARNG information system security testing requirements. Prepare, at a minimum, two ST&E Test Plans and supporting the resulting testing activities during the life of the contract.
f. Coordinate external system reviews (Agent for the Certificate Authority (ACA) teams) as necessary.
g. Maintain a record of accreditations and expiration dates, and report monthly or as directed by the Government on upcoming expiration of accreditations with an annual and six-month time horizon.
h. Provide C&A support to other ARNG systems accreditations. (*This service is expected to be required in CY2016.)*
i. Perform RMF assessments of existing and new, state and NGB systems seeking ATO. (*This service is expected to be required in CY2016*.)

C.5.5.3.14 SUBTASK 3.14 – CYBERSECURITY/NETWORK DEFENSE TOOLS SUPPORT

The contractor shall:

a. Provide HBSS support including:
   1. Manage, maintain, and operate Super Agent Distributed Repository (SADR) servers.
   2. Manage, maintain, and operate ePolicy Orchestrator (ePO) enterprise directory to ensure state systems can communicate with ePO.
   3. Coordinate the deployment of HBSS modules to the states and territories.
   4. Upgrade HBSS modules.
   5. Provide Tier II/III support for modules.
   6. Report on HBSS compliance and issues.
b. Provide ACAS support including:
   1. Manage the Security Center application and OS to ensure compliance with Army requirements.
   2. Support state installation and upgrades.
   3. Troubleshoot state scanning and results.
   4. Monitor ACAS system and correct any problems.
   5. Provide ad hoc, daily, and weekly reporting of state scanning and the quality of those scans.
   6. Provide a weekly reporting of ACAS findings and the remediation status.
c. Provide IPS/IDS support including:
   1. Monitoring and tuning of IPS signatures.
   2. Upgrade and maintain managers and sensors.
   3. Implement custom rules based on cyber intelligence provided by ARCYBER or other agencies.
   4. Monitor events sent to Arcsight.
d. Provide Firewall support including:
   1. Create and update firewall rules to accommodate access to appropriate data sources.
   2. Support firewall port activation by validating entries into DISA’s Ports, Protocols and Service Management (PPSM) registry.
   3. Provide assistance to states with PPSM submissions and validate state application information in the PPSM registry.

C.5.5.3.15 SUBTASK 3.15 - COMPUTER NETWORK DEFENSE TEAM (CNDT) SUPPORT

The EOSS RCC-NG monitors and reports on security events within the network. The contractor shall:

a. Provide computer/network incident response capabilities to detect, analyze, and respond to Computer Network Defense (CND) incidents.
b. Support and comply with Government-directed CND Response Actions (RAs). The contractor shall identify, monitor, comply with, and respond to CND RAs, based on intelligence reporting, active network incidents, or trends.
c. Provide immediate support to serious incidents, intrusions, or compromises (classified spillage, unauthorized intrusion, or virus outbreak) IAW Army Regulation 25-2 (AR 25-2).
d. Provide cyber threat/issue recommendations/warnings/notifications, to mitigate or respond to threats and vulnerabilities, to the Government for validation and acceptance based on established policies. The urgency or phasing of any actions shall consider the level of threat or vulnerability to the network. In the case of an adverse impact, the contractor shall provide alternative actions to achieve the original intent of the CND-RAs.
e. Create and submit appropriate security-related reports, such as required by IAVA, intrusion, virus infection incidents, and others as requested by the customer.
f. Establish and execute procedures to isolate, analyze, and respond to detected threats.
g. Perform the following functions supporting the CNDT operations:
    1. Maintain a 24x7x365 incident/event handling capability.
    2. Give feedback in the form of post-incident analysis reports to subscribers.
    3. Perform vulnerability analysis and penetration tests.
    4. Collect and analyze network intrusion artifacts from a variety of sources to include logs, system images, and packet captures to enable mitigation of network incidents.
    5. Develop, review, and update procedures for reporting incidents to Law Enforcement and Counterintelligence (LE/CI) agencies.
    6. Respond to ongoing network compromises and/or attacks by making network defense recommendations.
    7. Perform trend analysis on incident data to identify common vulnerabilities and make recommendations for countermeasures, which are shared with Tier 2 and subscribers.
    8. Provide INFOCON support and update services via GKO site.
    9. Ensure system stability through the use of DoD-approved, Government-furnished, anti-virus software in server systems and maintain current versions of the security products available from the Army CNDT site at https://www.acert.1stiocmd.army.mil/or from the DoD Computer Emergency Readiness Team (CERT) at https://www.us-cert.gov/.
    10. Notify the COR and appropriate IMN Government personnel immediately in the event that a computer virus or virus-like activity is detected at the RCC-NG facility.
    11. Notify the COR and appropriate IMN Government personnel immediately in the event of an attempted or successful electronic or physical intrusion at the off-site facility.

C.5.5.3.16 SUBTASK 3.16 - COMMAND CYBER READINESS INSPECTION (CCRI) SUPPORT

The contractor shall:

a. Report State CCRI status, findings, and results.
b. Track CCRI findings that have POA&M and report status.
c. Support states undergoing CCRI inspections.
d. Attend weekly meetings of CCRI status before inspection.
e. Provide ad hoc scanning and patching of state assets.
f. Provide detailed ACAS reporting of CCRI status of states in the CCRI process.
g. Travel to locations designated for CCRI inspections to provide technical support on IA tools implementation at the request of the Government.

C.5.5.3.17 SUBTASK 3.17 – IT SERVICE BROKER

The contractor shall perform the following duties as IT Service Broker for those services that are provisioned by external entities:

a. Liaise between Enterprise IT Services and Support consumers and external service providers.
b. Advocate for ARNG with external entities ensuring mutual understanding of the unique and multifaceted mission of the NGB.
c. Analyze processes and service delivery to maximize efficiency.
d. Maintain current service levels and monitor external service providers to ensure provided services are being delivered IAW previously agreed-to levels.
e. Research areas where internal services have the greatest potential for transition to external providers and report findings.
f. Transition from internally provided services to external providers by establishing relationships, creating a transition plans, documenting processes, drafting training materials, assisting in policy development, and ensuring continued successful transition.

Currently DISA Enterprise Email (DEE) and DoD Mobility (mobile access) are provided by DISA and data transport is provided by Army NETCOM. Cyber Security/IA tools are provided by other DoD partners. It is envisioned that, in the future, any services that move to a cloud-based solution and the alignment with the Joint Information Environment (JIE) will require IT Service Broker support.

C.5.5.4 SUBTASK 4 - GOVERNMENT FURNISHED EQUIPMENT (GFE)

The ARNG will provide the contractor with GFE that operates the EOSS. The contractor shall be responsible for the accountability, operations and management (O&M), and lifecycle management of the GFE.

C.5.5.4.1 SUBTASK 4.1 - GFE ACCOUNTABILITY AND MANAGEMENT

The contractor shall:

a. Adhere to asset and configuration processes.
b. Perform duties as the primary hand receipt holder (HRH) IAW AR 710-2 and AR 735-2 to the ARNG Property Book Office (PBO) for GFE under the EOSS TO's control. The contractor must comply with all FAR, Defense Federal Acquisition Regulation Supplement (DFAR), DoD, Army and NGB regulations, guidelines, and procedures governing GFE. The contractor shall perform regular inventories that are validated against Government SLAs.
c. Perform physical asset audits to validate inventory IAW DoD, Army, and NGB regulations, guidelines, and procedures and prepare an Asset Audit Report (**CDRL 05**) (**Section F, Deliverable 26**). The Asset Audit Report shall include:
    1. Hardware data elements including, but not limited to:
        A. Accountable Unit Identification Code (UIC) (if available)
        B. Asset Class
        C. Asset Status
        D. Asset Type
        E. Building
        F. Floor
        G. Machine Name
        H. Manufacturer
        I. Model
        J. Asset Tag
        K. Parent Asset Tag
        L. Parent Serial Number
        M. Site Code
        N. Rack
        O. Room
        P. Row
        Q. Serial Number
        R. Slot
    2. Software data elements including, but not limited to:
        A. License Key
        B. License Name
        C. License Serial Number
        D. Number of Actual License Distributions
        E. Number of License Entitlements
        F. Manufacturer

G. Manufacturing Part Number
H. Software Application Name
I. Current Software Application Version on the Network
J. License Type (e.g., perpetual or term)
K. Asset Status
L. Vendor (e.g., reseller or GFP)
M. Maintenance Contract Number.

d. Maintain GFE information in the CMDB.
e. Report GFE management activities in the MPSR.

C.5.5.4.2 SUBTASK 4.2 - EQUIPMENT DISPOSITION

All obsolete, excess, or surplus equipment, hardware, and software at contractor or Government facilities shall be properly disposed of by the contractor IAW applicable laws and regulations.

The contractor shall:

a. Adhere to ARNG PBO guidance for disposition of obsolete (or no longer needed) GFE.
b. Update repositories of record.
c. Report activities in MPSR.

C.5.5.4.3 SUBTASK 4.3 - GFE MAINTENANCE AND AGREEMENTS

GFE and Government-Furnished Software (GFS) all require warranty and maintenance contracts. To mitigate service disruptions, all GFE shall remain covered by maintenance agreements throughout its deployment, as well as receive proactive notification of any future maintenance coverage requirements.

The contractor shall:

a. Procure the GFE and GFS maintenance on a cost-reimbursable basis. (See **Section J, Attachment JJ** for a list of the current agreements.)
b. Provide the following required services:
    1. Manage all equipment and systems maintenance support agreements, unless directed otherwise by the ARNG.
    2. Maintain accurate maintenance agreements information in the CMDB.
c. Track, manage, and report GFE warranties and maintenance agreements.

C.5.5.4.4 SUBTASK 4.4 - SITE EQUIPMENT SUPPORT

All of the GuardNet equipment is located in Government facilities, typically co-located with the state, territory, and DC JFHQs. As such there are typically Government employees that can provide touch-labor support. In the case that Government support is unavailable or lacks the

necessary skill sets, the contractor shall provide touch labor support and materials to perform fix and upgrade activities on-site at all ARNG GuardNet locations. (See **Section J, Attachment KK** for historical list for these activities.)

The contractor shall:

a. Provide on-site maintenance, fix, and upgrade support as required to include:
    1. Maintaining operational capabilities of the Enterprise systems as part of activities associated with support.
    2. In order to maintain appropriate on-site support, the contractor shall perform the following tasks:
        A. Determination that equipment, or its parts, need to be repaired or replaced.
        B. Ordering of appropriate parts.
        C. Configuration.
        D. Shipment to site.
        E. On-site installation, including scheduling with site personnel.
        F. Testing.
        G. Disposal of old parts.
        H. Updates to the information in the CMS.
b. Coordinate all logistics and schedules associated with on-site visits and repairs.
c. Provide the Government with monthly updates concerning the fix and maintenance activities.
d. Perform RCC-NG on-site support during the hours of 6 AM to 6 PM Monday through Sunday geographical local time; however, the contractor shall also provide after-hour support, if required by the local conditions.

C.5.5.5 SUBTASK 5 - SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) CONNECTIVITY

ARNG requires a SIPRNet connectivity to the contractor's RCC-NG facility. The RCC-NG (i.e., the NOSC space) will be a closed space.

The contractor shall:

a. Ensure that the RCC-NG facility supports all requirements for establishing SIPRNet connectivity IAW National Industrial Security Program Operating Manual (NISPOM) 5220.22-M.
b. Provide a closed space RCC-NG with the capabilities for secure Video Teleconference (VTC) for up to six to seven people.
c. Prepare a Security Accreditation Package sufficient to be approved by Defense Security Services (DSS). This includes, but is not limited to, demonstrating conformance with the following:

1. DoD 8510.01 Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) to be transitioned to the Department of Defense Information Assurance Risk Management Framework (DIARMF) once Army implements the change.
2. DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) for connections between DoD and contractor information Systems.
3. DoDI 8551.1 Ports, Protocols, and Services Management (PPSM).
4. CJCSI 6211.02C DISN Policy and Responsibilities.
5. DISN Connection Process Guide (CPG).

C.5.6 TASK 6 – PROJECT AND INITIATIVE SUPPORT (OPTIONAL)

The contractor shall provide support for ARNG requirements and systems in the form of short-term projects and initiatives and for unanticipated requirements including system, system component, or application failure; systems integration; systems deployment; DoD and Congressional mandates, project management support, data warehouse support; help desk, service desk, or call center support; desktop support; and unanticipated requirements.

Examples of projects and initiatives are:

a. Government Directive Initiatives (GDIs). GDIs are those that are either requested by the Government or proposed by the contractor and approved by the ARNG. These initiatives may be implemented in response to special needs that arise due to changing ARNG requirements or needs driven by major industry developments, changing technologies, or DoD directives. The ARNG will provide the contractor with the requirements of these tasks and will work with the contractor in managing the work progress.
b. Refresh of the GuardNet equipment. It is estimated that new hardware/software will begin to be supplied by the Government at various ARNG locations in July or August of 2015. The contractor shall remotely configure the new hardware/software in the various sites. All equipment shall be Energy Star Compliant IAW Far Clause 52.223-15 as contained in **Section I** of the TOR.
c. At an unknown point-in-time during the life of the TO, the Government may require the contractor to move operations from the COCO RCC-NG to a Government-supplied facility.
d. The contractor shall assist with the consolidation of the NGB SIPRNet connections in GuardNet-S.
e. The ARNG has several ITSM projects the contractor shall support. Some are ongoing and others are projected (see **Section J, Attachment W**). The contractor shall assist by remotely configuring the new capabilities for the each set of users in the referenced state locations.
f. A previous upgrade of the Windows Server OS to Windows 2008 R2 (this was a security mandate).
g. A previous upgrade of the ALT-NOSC (alternative NOSC) equipment.
h. The ARNG plans to move the RCC-NG operations along with all the associated staff and SPPN equipment to its Government Readiness Center campus in Arlington, Virginia, or

other Government facility. The contractor shall develop a physical relocation plan and an approach for transitioning to Government facilities. The contractor shall relocate personnel, EOSS services and required equipment, data circuits and phone access, and operations to the designated Government facility. The contractor shall ensure continuity of operations during the relocation.

The contractor shall provide appropriate technical and project management personnel to fulfill the requirements of these specific tasks.

C.5.7 TASK 7 – TECHNICAL REFRESH SUPPORT

The contractor shall refresh the equipment, software, and tools on an incremental basis over a three- to five-year period (See S**ection J, Attachment V** - GFE Inventory List (hardware and software)). The contractor shall purchase the items, including maintenance agreements, manage and test the items, and then ship them to required destination. The contractor shall provide remote help desk support during and after the installation. All equipment shall be Energy Star Compliant IAW Far Clause 52.223-15 as contained in **Section I** of the TOR.

C.5.8 TASK 8 - ACCOUNTING FOR CONTRACT SERVICES

The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collections site where the contractor shall report ALL contractor manpower (including subcontractor manpower) required for performance of this contract. The contractor is required to completely fill in all the information in the format using the following web address: https://cmra.army.mil. The required information includes:

a. Contracting Office, Contracting Officer (CO), COR.
b. Contract number, including task and delivery order number.
c. Beginning and ending dates covered by reporting period.
d. Contractor name, address, phone number, and e-mail address, and identity of contractor employee entering data.
e. Estimated direct labor hours (including subcontractors).
f. Estimated direct labor dollars paid in the reporting period (including subcontractors).
g. Total payments (including subcontractors).
h. Predominant Federal Service Code (FSC) reflecting services provided by the contractor (separate predominant FSC for each subcontractor if different).
i. Estimated data collection costs.
j. Organizational title associated with the UIC for the Army Requiring Activity (the Army requiring Activity is responsible for providing the contractor with its UIC for the purposes of reporting this information.
k. Locations where contractor and subcontractor perform the work (specified by zip code in the U.S. and nearest city and country (when in overseas locations) using standardized nomenclature on website.
l. Presence of deployment or contingency contract language.

m. Number of contractor and subcontractor employees deployed in theater during the reporting period (by country).

As part of its submission, the contractor shall also provide the estimated total cost (if any) incurred to comply with this reporting requirement. The reporting period will be the period of performance, NTE 12 months, ending September 30 of each Government Fiscal Year (FY) and must be reported by October 31 of each calendar year or at the end of the contract, whichever comes first. Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

SECTION D - PACKAGING AND MARKING

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

SECTION E - INSPECTION AND ACCEPTANCE

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

E.2 PLACE OF INSPECTION AND ACCEPTANCE

The ARNG TPOC and the FEDSIM COR shall perform inspection and acceptance of all work performance, reports, and other deliverables under this TO.

E.3 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR and the ARNG TPOC. Inspection may include validation of information or software through the use of automated tools, testing, or inspection of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.4 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO, the contractor's proposal, and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected IAW the applicable clauses.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, and/or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables must either be incorporated in the succeeding version of the deliverable, or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the requirements stated within this TO, the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FEDSIM COR.

E.5 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in **Section F**) from Government receipt of the

draft deliverable. Upon receipt of the Government's comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.6 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The CO/COR will provide written notification of acceptance or rejection (**Section J, Attachment I**) of all final deliverables within 15 workdays (unless specified otherwise in **Section F**). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.7 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

For FFP tasks:
If the contractor does not provide products or services that conform to the requirements of this TO, the Government will not pay the fixed price associated with the non-conforming products or services.

For CPAF tasks:
If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the award fee determination report, and there will be an associated reduction in the earned award fee.

SECTION F – DELIVERABLES OR PERFORMANCE

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

F.3 TASK ORDER PERIOD OF PERFORMANCE

The period of performance for this TO is a one-year base period and four, one-year options.

F.4 PLACE OF PERFORMANCE

Place of Performance is the contractor-provided facility used to house and manage the NOC/SOC. Occasional access to the Arlington Hall Station (AHS) is needed to maintain the GuardNet equipment located there and occasionally access to the alternative site at Camp Robinson could be required. At an unknown time during the life of the TO, the primary place of performance may move to a Government site. Occasional long-distance travel is anticipated to be required in support of this effort.

F.5 DELIVERABLES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

NLT: No Later Than
TOA: Task Order Award
PS: Project Start
IAW: In Accordance With
All references to Days: Government Workdays unless otherwise stated

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The estimated TOA date for proposal purposes is October 2015 which determines PS to be February 1, 2016 based on the deliverable schedule below. These dates are for proposal purposes only.

The contractor shall submit the deliverables listed in the following table:

DELIVERABLE NUMBER	MILESTONE/DELIVERABLE	TOR REF.	PLANNED COMPLETION DATE
	Project Start (PS)		Feb. 1, 2016
01	Integrated Master Schedule (IMS) (**CDRL 04**)	C.5.1.1	PS + 10 days
02	Project Kick-Off Meeting	C.5.1.2	PS + 5 days
03	Technical Status Meeting (**CDRL 03**)	C.5.1.4	As required
04	Draft PMP (**CDRL 01**)	C.5.1.5	PS + 14 days

SECTION F – DELIVERABLES OR PERFORMANCE

DELIVERABLE NUMBER	MILESTONE/DELIVERABLE	TOR REF.	PLANNED COMPLETION DATE
05	Final PMP (**CDRL 01**)	C.5.1.5	Draft submission + 25 days
06	Daily System Status Report (Reports **CDRL 05**)	C.5.1.6.1	Daily
07	Weekly System Status Report (**CDRL 05**)	C.5.1.6.2	Weekly
08	Monthly Program Status Report (MPSR) (**CDRL 05**)	C.5.1.6.3	Monthly IAW PMP
09	Trip Reports (Reports **CDRL 05**)	C.5.1.7	As required
10	Final QCP	C.5.1.8	PS + 14 days
11	Risk Management Plan (**CDRL 06**)	C.5.1.9	IAW PMP
12	Standard Operating Procedures (SOPs)	C.5.1.12	14 days after completion of transition
13	IT Service Management Plan Updates (**CDRL 08**)	C.5.4	IAW PMP
14	Final Transition-In Plan	C.5.2	PS + five days
15	Transition-Out Plan (**CDRL 07**)	C.5.3	120 calendar days after option exercised
16	Baseline Technology and Tool Assessment Report (**CDRL 05**)	C.5.4.1	IAW PMP
17	CSI Register (Service Improvement Plan) (**CDRL 09**)	C.5.4.1	IAW PMP
18	Technology Trending Reports (**CDRL 05**)	C.5.4.2.2	IAW PMP
19	Operational Level Agreements (OLAs) (**CDRL 10**)	C.5.4.3.1.1	IAW PMP
20	Disaster Recovery Plan (**CDRL 12)**	C.5.4.3.1.5	IAW PMP
21	After Action Report (AAR) (**CDRL 05**)	C.5.4.3.1.5	As required
22	Service Design Packages (**CDRL 13**)	C.5.4.3.2.2	As required
23	Configuration Audits (**CDRL 05**)	C.5.4.4.1.1	IAW PMP
24	CND Impact Report and Recommendations	C.5.5.3	As required
25	Security Test and Evaluation (ST&E) Test Plan (**CDRL 15**)	C.5.5.4.14.2	IAW PMP
26	Asset Audit Report (**CDRL 05**)	C.5.5.5.1	IAW PMP
27	Fully Executed Redacted Task Order Document	F.5.1	At PS

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-confirming markings IAW subparagraphs (e) and (f) of the FAR clause at 52.227-14.

SECTION F – DELIVERABLES OR PERFORMANCE

F.5.1 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the Fully Executed Redacted Task Order Document (**Section F, Deliverable 27**) with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall demonstrate why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under the FOIA.

GSA will carefully consider all of the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5.2 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by email and removable electronic media, as well as place them in the ARNG GKO (SharePoint) repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

• Text	MS Word
• Spreadsheets	MS Excel
• Briefings	MS PowerPoint
• Drawings	MS Visio
• Schedules	MS Project

F.6 PLACE(S) OF DELIVERY

Unclassified deliverables and correspondence shall be delivered to the GSA CO or COR at the following address:

GSA FAS AAS FEDSIM
ATTN: Danton F. Jennings, COR

1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405

Telephone: (703) 605-3640
Email: danton.jennings@gsa.gov

Copies of all deliverables shall also be delivered to the ARNG TPOC:

Provided after award.

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) (**Section J, Attachment H**) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

SECTION G – CONTRACT ADMINISTRATION DATA

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

G.3.5 CONTRACTING OFFICER'S REPRESENTATIVE

The CO will appoint a COR in writing through a COR Appointment Letter (**Section J, Attachment A**). The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

G.3.5.1 CONTRACT ADMINISTRATION

Contracting Officer:

Michael Chappelle
GSA FAS AAS FEDSIM

1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (703) 605-2656
Email: michael.chappelle@gsa.gov

Contracting Officer's Representative:

Danton F. Jennings
GSA FAS AAS FEDSIM

1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (703) 605-3640
Email: danton.jennings@gsa.gov

Technical Point of Contact:

Provided after award.

G.9.6 INVOICE SUBMISSION

The contractor shall submit Requests for Payments IAW the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV

2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice.

Task Order Number: GSQ0016AJ0009
Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*
FEDSIM Project Number: AR00702
Project Title: Enterprise Operations and Security Services (EOSS)

The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The contractor shall provide invoice backup data IAW the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information SysTem (ASSIST) to submit invoices. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Log in using your assigned ID and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the Create New Invoice button. The AASBS Help Desk should be contacted for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

G.9.6.1 INVOICE REQUIREMENTS

The contractor may invoice the fixed fee on a monthly basis. The monthly fixed fee invoiced shall be proportionate to the amount of labor expended for the month invoiced.

The contractor shall submit a draft or advance copy of an invoice to the client point of contact for review prior to its submission to GSA.

If the TO has different contract types, each should be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion.

G.9.6.1.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in **Section B**), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees).
b. Employee company labor category.
c. Employee Alliant labor category.
d. Monthly and total cumulative hours worked.
e. Corresponding TO proposed rate (as proposed in the cost proposal).
f. Cost incurred not billed (by Task Area).
g. Current approved forward pricing rate agreement in support of indirect costs billed.

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges and shall also include the Overhead and General and Administrative rates being applied.

The contractor may invoice after accepting the modification which includes the award fee determination and any corresponding deobligation of unearned fee. See the Award Fee Determination Plan in **Section J, Attachment E** for additional information on the award fee determination process.

G.9.6.1.2 FIRM-FIXED-PRICE (FFP) CLINs (for LABOR)

The contractor may invoice as stated in **Section B** for the FFP CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All costs shall be reported by CLIN element (as shown in **Section B**) and shall be provided for the current invoice and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. FFP period of performance– as stated in **Section B.**

G.9.6.1.3 TOOL PURCHASES AND OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the ODCs and Tools purchased. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. Tools and/or ODCs purchased.
b. Consent to Purchase number or identifier.
c. Date accepted by the Government.
d. Associated CLIN.
e. Project-to-date totals by CLIN.
f. Cost incurred not billed.
g. Remaining balance of the CLIN.

All cost presentations provided by the contractor shall also include Overhead charges, General and Administrative charges, and Fee.

G.9.6.1.4 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

- Joint Travel Regulation (JTR) - prescribed by the GSA, for travel in the contiguous U.S.
- Federal Travel Regulation (FTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR. The invoice shall include the period of performance covered by the invoice, the CLIN number, and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period's travel details shall include separate columns and totals and include the following:

a. Travel Authorization Request number or identifier, approver name, and approval date.
b. Current invoice period.
c. Names of persons traveling.
d. Number of travel days.
e. Dates of travel.
f. Number of days per diem charged.
g. Per diem rate used.
h. Total per diem charged.
i. Transportation costs.
j. Total charges.
k. Explanation of variances exceeding 10% of the approved versus actual costs.
l. Indirect Handling Rate.

SECTION G – CONTRACT ADMINISTRATION DATA

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

H.2 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO. The contractor may augment its "Key" team with additional Key Personnel as appropriate to its solution.

a. Program Manager (PM)
b. Service Design Manager
c. Service Operations Manager
d. Service Transition Manager
e. Cyber Security Manager
f. Network Services Manager
g. Tools Engineer Lead
h. Change Manager

The Government desires that Key Personnel be assigned for the duration of the TO. When referring to a "relevant degree" in the desirable qualifications below, the following are considered examples of relevant degrees - Computer Science, Information Systems, Information Technology, Cyber Security, Statistics, Business Administration, Systems Engineering, Computation Science, Computer Engineering, Electrical Engineering, Data Analytics, Information Technology, Information Security and Assurance, Mathematics, Software Engineering, Systems Engineering, and Telecommunications.

H.2.3 PROGRAM MANAGER (PM)

The PM shall serve as the contractor's single TO manager and shall be the contractor's authorized interface with the Government CO, COR, and TPOC for the TO.

It is required that the PM have the qualifications/certifications listed below (see **Section M.6.3 (a)**):

a. An active Project Management Institute (PMI) Project Management Professional (PMP®) or PMI Program Management Professional (PgMP®) Certification, or equivalent at the time of proposal submission.
b. An ITIL 2007/2011 Intermediate Level Certification. Please state related exam/exams.
c. Information Assurance Management (IAM) Level I.

It is desirable that the PM has the following qualifications as a contract/TO PM:

a. Experience managing, as a PM, on a Federal TO/contract requiring transition of infrastructure and operations to a COCO facility.

b. Experience managing, as a PM, on a Federal TO/contract providing continual service improvements similar to the requirements of the TOR.
c. Experience managing, as a PM, on a Federal TO/contract providing managed services similar to the requirements of the TOR.
d. Experience managing, as a PM, on a Federal TO/contract on a CPAF basis for services similar to the requirements of the TOR.
e. A relevant educational degree (see **Section H.2**).

H.2.4 SERVICE DESIGN MANAGER

The Service Design Manager is responsible for service delivery of processes that fall in the Service Design area of the ITIL process model such as Service Level Management, IT Service Continuity, Capacity Management, Service Catalog Management. The Service Design Manager shall manage the IMS, resourcing for all projects and coordination of projects with internal and external stakeholders.

It is required that the Service Design Manager have the qualifications/certifications listed below (see **Section M.6.3 (a)**):.

a. An Information Assurance Technical (IAT) Level III or IAM Level III.
b. ITIL 2007/2011 Intermediate Level Certification. Please state related exam/exams.

It is desirable that the Service Design Manager has the following qualifications as a contract/TO Service Design Manager:

a. Experience managing the design of and implementation of ITIL service improvements over time, similar to those of the TOR.
b. Experience developing long-range plans for delivery of IT services.
c. Experience reducing TCO utilizing ITIL mechanisms.
d. A relevant educational degree (see **Section H.2**).

H.2.5 SERVICE OPERATIONS MANAGER

The Service Operations Manager shall be responsible for service delivery of processes that fall in the Service Operations area of the ITIL and process model management, such as Event Management, Problem Management, Access Management, and Request Fulfillment. The Service Operations Manager shall also be responsible for Enterprise IT Services and Support such a Service Desk, WAN and LAN management, and VOC.

It is required that the Service Operations Manager have the qualifications/certifications listed below (see **Section M.6.3 (a)**):

a. An IAT Level III or IAM Level III.
b. An ITIL 2007/2011 Intermediate Level Certification. Please state related exam/exams.

It is desirable that the Service Operations Manager has the following qualifications as a contract/TO Service Operations Manager:

a. Experience managing service operations, as a service manager, against SLAs on a DoD TO/contract on a CPAF basis.
b. Experience managing and improving service availability and capacity management in a network environment similar to the requirements of the TOR.
c. A relevant educational degree (see **Section H.2**).

H.2.6 SERVICE TRANSITION MANAGER

The Service Transition Manager shall be responsible for service delivery of processes that fall in the Service Transition area of the ITIL process model such as Service Asset and Configuration Management, Release and Deployment Management, Change Management, and Knowledge Management, as well as preparing changes for release into operations.

It is required that the Service Transition Manager have the qualifications/certifications listed below (see **Section M.6.3 (a)**):

a. IAM Level I.
b. An ITIL 2007/2011 Intermediate Level Certification. Please state related exam/exams.

It is desirable that the Service Transition Manager has the following qualifications as a contract/TO Service Transition Manager:

a. Experience transitioning to a COCO facility with infrastructure and security constraints similar to the requirements of the TOR.
b. Experience transitioning improved services with underpinning infrastructure and tools based on ITIL principles.
c. A relevant educational degree (see **Section H.2**).

H.2.7 CYBER SECURITY MANAGER

The Cyber Security Manager shall be responsible for all areas of IT security/Information Assurance and assist the Information Assurance Program Manager (IAPM) in managing the risk of operating a large network including CND, HBSS, and C&A support and tracking.

It is required that the Cyber Security Manager have the qualifications/certifications listed below (see **Section M.6.3 (a)**):

a. An IAM Level III Certification.
b. Experience managing cyber security for a DoD agency with requirements and infrastructure/tools similar to those of the TOR.

c. ITIL 2007/2011 Foundation Level Certification. Please state related exam/exams.

It is desirable that the Cyber Security Manager has the following qualifications as a contract/TO Cyber Security Manager:

a. Experience managing and using the Cyber tools that are referenced in the TOR.
b. A relevant educational degree (see **Section H.2**).

H.2.8 NETWORK SERVICES MANAGER

The Network Services Manager shall be responsible for Enterprise IT Services and Support such as the Regional Cyber Center-National Guard/Service Desk, WAN and LAN operations.

It is required that the Network Services Manager have the qualifications/certifications listed below (see **Section M.6.3 (a)**):

a. An IAT Level III or IAM Level III.
b. ITIL 2007/2011 Foundation Level Certification. Please state related exam/exams.

It is desirable that the Network Services Manager has the following qualifications as a contract/TO Network Services Manager:

a. Experience managing network services for a similar network platform to that of the current EOSS environment.
b. Experience operating and maintaining network services for COOP sites similar to the requirements of the TOR.
c. A relevant educational degree (see **Section H.2**).

H.2.9 TOOLS ENGINEER LEAD

The Tools Engineer Lead shall be responsible for all tools used to manage GuardNet and Enterprise IT Services and Support as well as the Enterprise Lab.

It is required that the Tools Engineer Lead have the qualifications/certifications listed below (see **Section M.6.3 (a)**):

a. An IAT Level III or IAM Level III.

It is desirable that the Tools Engineer Lead has the following qualifications as a contract/TO Tools Engineer Lead:

a. Experience using the tools provided by the Government as GFE.
b. Experience engineering tool solutions that provide operational efficiencies and TCO improvements in an environment similar to the TOR.

c. A relevant educational degree (see **Section H.2**).

H.2.10 CHANGE MANAGER

The Change Manager shall be responsible for managing change processes, including tools, maintaining the change schedule and interfacing with other process/service owners/managers of GuardNet services.

It is required that the Change Manager have the certifications listed below (see **Section M.6.3 (a)**):

a. ITIL 2007/2011 Intermediate Level Certified. Please state related exam/exams.

It is desirable that the Change Manager has the following qualifications as a contract/TO Change Manager:

a. Experience managing change processes providing managed services similar to the requirements of the TOR.
b. A relevant educational degree (see **Section H.2**).

H.2.11 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in the proposal in response to the TOR, the contractor shall notify the Government CO and the COR of the existing TO. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category(ies) of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6, Termination (Cost Reimbursement) or FAR 52.249-8, Default (Fixed-Price Supply and Service).

H.5 GOVERNMENT-FURNISHED EQUIPMENT (GFE)

The ARNG will provide the contractor with GFE that operates the EOSS services to include what is needed for the LAN. The contractor shall be responsible for the accountability, operations and management (O&M), and lifecycle management of the GFE. See **Section J, Attachment V** for a complete list.

H.5.2 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will provide the information listed in the **Section J** of the TOR with the solicitation, also listed below:

a. GFE Inventory List (hardware and software).
b. Enterprise IT Services and Support Portfolio.
c. Status of Long-Range Plans.
d. Service Level Agreements (SLAs).
e. Service Level Objectives.
f. List of ARNG Support Contractors.
g. Examples of Government Directed Initiatives.
h. EOSS Service Catalog.
i. GuardNet Wide Area Network Routing Design.
j. ARNG State Service Levels.
k. Historical Service Statistics and Metrics.
l. Current Government-Furnished Equipment and Government-Furnished Software Maintenance Agreements.
m. Historical List of Touch Labor Support and Materials.

H.7 SECURITY CONSIDERATIONS

The contractor shall comply with the following security constraints based on the Draft DD 254 in **Section J, Attachment C** applied to **Sections H.7.2** and **H.7.3**. **Section H.7.4** provides a list of security considerations/requirements that the contractor personnel must follow when performing on this Task Order.

H.7.2 INFORMATION ASSURANCE

At all times, the contractor shall be in compliance with the following requirements that are contained in Table 1 for the DoD 8570.01 mandate: INFORMATION ASSURANCE WORKFORCE IMPROVEMENT PROGRAM (January 2012).

a. The contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions IAW DoD 8570.01-M, Information Assurance Workforce Improvement Program. The contractor shall meet the applicable information assurance certification requirements, including-
    1. DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M.
    2. Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

b. The contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions and upload in the appropriate database.
c. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.
d. Document the approach to meeting personnel DoD 8750.01-M compliance in the Staffing Plan.

H.7.3 SECURITY CLEARANCES

The contractor shall ensure that all personnel assigned to the execution of this TO meet the minimum of DoD Secret security clearance requirements IAW AR 25-2 for Information Assurance and NISPOM.

H.7.4 ACCESS CONDITIONS AND CONSTRAINTS

The contractor shall comply with the following:

Facility conditions:

a. Unscheduled gate closures by the Security Police may occur at any time causing all personnel entering or exiting a closed installation to experience a delay. This cannot be predicted or prevented. Contractors are not compensated for unexpected closures or delays. Vehicles operated by contractor personnel are subject to search pursuant to applicable regulations. Any moving violation of any applicable motor vehicle regulation may result in the termination of the contractor employee's installation driving privileges.

b. The contractor's employees shall become familiar with and obey the regulations of the installation; including fire, traffic, safety and security regulations while on the installation. Contractor employees should only enter restricted areas when required to do so and only upon prior approval. All contractor employees shall carry proper identification with them at all times. The contractor shall ensure compliance with all regulations and orders of the installation which may affect performance.

Security Requirements:

The contractor shall comply with all applicable installation/facility access and local security policies and procedures, which may be obtained from the Government. The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. The contractor shall ensure compliance with all personal identity verification requirements as directed by DOD, HQDA and/or local policy. Should the Force Protection Condition (FPCON) change, the Government may require changes in contractor security matters or processes.

a. **COMSEC/IT Security.** All communications with DOD organizations are subject to communications security (COMSEC) review. All telephone communications networks are continually subject to intercept by unfriendly intelligence organizations. DOD has authorized the military departments to conduct COMSEC monitoring and recording of telephone calls originating from, or terminating at, DOD organizations. Therefore, the contractor is advised that any time a contractor places or receives a call it is subject to COMSEC procedures. The contractor shall ensure wide and frequent dissemination of the above information to all employees dealing with DOD information. The contractor shall abide by all Government regulations concerning the authorized use of the Government's computer network, including the restriction against using the network to recruit Government personnel or advertise job openings.

b. Use of Government Information Systems (IS) and access to Government networks is a revocable privilege, not a right. Users are the foundation of the DoD strategy and their actions affect the most vulnerable portion of the AEI. Contractor employees shall have a favorable background investigation or hold a security clearance and access approvals commensurate with the level of information processed or available on the system. Contractor employees shall:

1. Comply with the command's Acceptable Use Policy (AUP) for Government owned IS and sign an AUP prior to or upon account activation.
2. Complete initial and/or annual Information Assurance (IA) training as defined in the IA Best Business Practices (BBP) training (https://informationassurance.us.army.mil).
3. Mark and safeguard files, output products, and storage media per classification level and disseminate them only to individuals authorized to receive them with a valid need to know.
4. Protect IS and IS peripherals located in their respective areas in accordance with physical security and data protection requirements.
5. Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.

c. **Protection of Personally Identifiable Information (PII).** The contractor shall protect all Personally Identifiable Information (PII) encountered in the performance of services in accordance with DFARS 224.103 and DoDD 5400.11, Department of Defense Privacy Program, and DoD 5400.11-R. If a PII breach results from the contractor's violation of the aforementioned policies, the contractor shall bear all notification costs, call-center support costs, and credit monitoring service costs for all individuals who's PII has been compromised.

d. **CAC Requirements.** The Common Access Card (CAC) is the Department of Defense (DOD) Federal Personal Identity Verification (PIV) credential. In accordance with Directive Type Memorandum (DTM) 08-003, December 1, 2008, incorporating Change 5, October 8, 2013, Initial issuance of a CAC requires at a minimum, the completion of FBI fingerprint check with favorable results reflecting "No Record" and submission of a National Agency Check with Inquiries (NACI) to the Office of Personnel Management

(OPM), or a DoD-determined equivalent investigation. The issuance of a CAC will be based on four criteria; (1) eligibility for a CAC; (2) verification of DoD affiliation from an authoritative data source; (3) completion of background vetting requirements according to the Federal Information Processing Standards Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006, and DOD Regulation 5200.2-R, Department of Defense Personnel Security Program, January 1987, and (4) verification of a claimed identity. CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting System (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Trusted Associate Sponsorship System (TASS).

1. **Trusted Associate Sponsorship System (TASS).** The contractor is responsible for processing applications for Common Access Cards (CAC) for every contractor employee who deploys with the military force OR who has need to access any Government computer network in accordance with FAR 52.204-9, "Personal Identity Verification of Contractor Personnel."

   The contractor is responsible for managing requests for new or renewal CAC cards in sufficient time to ensure that all contractor employees have them when needed to perform work under this contract. The norm is at least ten calendar days advance notice to the Trusted Agent (TA), unless there are extenuating circumstances approved by the Government.

   The contractor shall obtain an Army Knowledge Online (AKO) email address for each applicant, including subcontractors, who may be deployed or require logical access to a government computer network. This can be done by going to: http://www.us.army.mil and register as an "Army Guest," with the sponsor being a Government designated individual to serve as an AKO Sponsor. **Note:** If an employee of a contractor loses the Privilege to access AKO, they lose the ability to renew their CAC. Therefore it is critical that contractor employees maintain their AKO accounts.

   It is recommend that a "Corporate Facility Security Officer" (FSO) be designated to serve as the contractor's single point of contact for Background Investigation (BI), the TASS application process and other CAC and security related matters. If a FSO is not established, each contractor employee requiring a CAC will be required to process their own applications.

   CAC applications shall be processed through the TASS. The contractor's FSO or contractor employee shall submit requests for a CAC via email to the designated TASS Trusted Agent (TA) before accessing the TASS website. The TASS TA for this requirement will be:

   The Government will establish a TASS application account for each CAC Request and will provide each contractor employee a USER ID and Password, via email, to the FSO. The FSO or contractor employee shall access the TASS account and

complete the CAC application (entering/editing contractor information as applicable) at: https://www.dmdc.osd.mil/tass/.

The FSO or contractor employee will submit completed applications in TASS and will follow up to ensure that the TA is processing the request.

A CAC cannot be issued without evidence that the FSO has initiated a National Agency Check with Written Inquires (NACI).

The Government will inform the contractor's applicant, via email, of one of the following:

A. Approved.* Upon approval, the information is transferred to the Defense Enrollment Eligibility Reporting System (DEERS) database and an email notification is sent to the contractor with instructions on obtaining their CAC. The contractor proceeds to a Real-Time Automated Personnel Identification System (RAPIDS) station (RAPIDS Site Locator: http://www.dmdc.osd.mil/rsl/).
B. Rejected.* The Government, in separate correspondence, will provide reason(s) for rejection.
C. Returned. Additional information or correction to the application required by the contractor employee.

*The contractor shall maintain records of all approved and rejected applications.

At the RAPIDS station, the RAPIDS Verification Officer will verify the contractor by SSN and two forms of identification. Identity source Documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, "Employment Eligibility Verification." Consistent with applicable law, at least one document from the Form I-9 list shall be a valid (unexpired) State or Federal Government-issued picture identification (ID). The Identity documents will be inspected for authenticity and scanned and stored in the DEERS upon issuance of an ID. The photo ID requirement cannot be waived, consistent with applicable statutory requirements. The Verification Officer will capture primary and alternate fingerprints, picture, and updates to DEERS and will then issue a CAC.

Issued CACs shall be for a period of performance not longer than three (3) years or the individual's contract end date (inclusive of any options), whichever is earlier.

The contractor shall return issued CAC's to the DEERS office upon departure or dismissal of each contractor employee. Obtain a receipt for each card and provide to the Government.

e. **AT Level 1 Awareness Training (AT).** All contractor employees requiring access to Army Installations, facilities, and controlled access areas shall complete Level 1 AT within 30 calendar days after contract start date and within 30 calendar days of new employees commencing performance. The contractor shall submit certificates of

completion for each affected contractor and subcontractor employee, within 15 calendar days after completion of training. Level 1 AT is available at https://jkodirect.jten.mil.

f. **Information Assurance (IA)/Information Technology (IT) Training.** All contractor employees shall complete the DoD IA Awareness Training before issuance of network access and annually thereafter. All contractor employees performing services involving IA/IT functions shall comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M and AR 25-2 within six months of the start of contract performance. In accordance with DoD 8570.01-M , DFARS 252.239.7001 and AR 25-2, contractor employees performing services supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M shall be completed upon contract award.

g. **Information Awareness.** All contractor employees with access to a government information system shall be registered in the ATCTS (Army Training Certification Tracking System) (https://atc.us.army.mil/iastar/index.php) prior to commencement of services, and shall successfully complete the DOD Information Assurance awareness training prior to access to the IS and then annually thereafter. (https://ia.signal.army.mil/DoDIAA/).

h. **WATCH Training.** The contractor with an area of performance within an Army-controlled installation, facilities or area shall brief all employees on the local iWATCH program. This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the Government. This training shall be completed within 30 calendar days of contract award and within 30 calendar days of new employees commencing performance. The contractor shall report completion for each affected contractor employee and subcontractor employee, to the Government, within 15 calendar days after completion of training.

i. **OPSEC Training.** In accordance with AR 530-1, Operations Security, new contractor employees shall complete Level I OPSEC training within 30 calendar days of their reporting for duty and annually thereafter. The contractor shall submit certificates of completion for each affected contractor employee, to theGovernment, within 15 calendar days after completion of training. Level 1 OPSEC training is available at http://cdsetrain.dtic.mil/opsec/.

j. **OPSEC SOP/Plan.** The contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan and provide it to the Government within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This SOP/Plan shall include the Government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. In addition, the contractor shall identify an individual who will be an OPSEC Coordinator. The contractor shall ensure this individual becomes OPSEC Level II certified in accordance with AR 530-1.

k. **Classified Information.** For Contracts That Require Handling or Access to Classified Information. The contractor shall comply with FAR Clause 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M) and applicable updates/changes. Secret is the security level for this contract; please see DD 254 for more information.

Physical Security:

The contractor shall safeguard all Government property provided for contractor use. At the close of each work period, Government facilities, equipment and materials shall be secured.

a. **Key Control.** The contractor shall establish and implement methods of ensuring all keys/key cards issued by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued by the Government shall be duplicated. (Add the following sentence is a QCP is required): Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The contractor shall immediately report any occurrences of lost or duplicated keys/key cards to the Government.

    1. In the event keys, other than master keys, are lost or duplicated, the contractor shall, upon direction by the KO, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due the contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the contractor.

    2. The contactor shall prohibit the use of the Government issued keys/key cards by any persons other than the contractor's employees. The contractor shall prohibit the opening of locked areas by contractor employees to permit entrance of persons other than contactor employees engaged in the performance of services in those areas, or personnel authorized entrance by the Government.

b. L**ock Combinations.** The contractor shall establish and implement methods of ensuring all lock combinations are not revealed to unauthorized persons. The contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations.

Special Qualifications:

Any contractors with elevated rights and privileges must comply with DD 8570.

H.9 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.9.1 ORGANIZATIONAL CONFLICT OF INTEREST

If the contractor has or is currently providing support or anticipates providing support to ARNG that creates or represents an actual or potential organizational conflict of interest (OCI), the contractor shall immediately disclose this actual or potential OCI IAW FAR Subpart 9.5. The contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the contractor (and any subcontractors, consultants, or teaming partners) agrees to disclose information concerning the actual or potential conflict with any proposal for any solicitation relating to any work in the TO. All actual or potential OCI situations shall be identified and addressed IAW FAR Subpart 9.5.

H.9.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form (**Section J, Attachment R**) and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are listed on a signed Addendum to the Corporate NDA Form (see **Section J, Attachment R**) prior to the commencement of any work on the TO.
b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information or source selection information.
c. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel also must be listed on a signed Addendum to the Corporate NDA and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.14 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 United States Code (U.S.C.) 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section

508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

H.16 COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS), affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and contract performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the contract/TO.

H.18 PURCHASING SYSTEMS

The objective of a contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting.

Prior to the award of the TO the CO shall verify the validity of the contractor's purchasing system. Thereafter, the contractor is required to certify to the CO no later than 30 calendar days prior to the exercise of any options the validity of its purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the contractor shall provide the results of the review to the CO within 10 workdays from the date the results are known to the contractor.

H.19 EARNED VALUE MANAGEMENT SYSTEM

The contractor shall employ EVM in the management of this TO IAW the American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard-748-A-1998, *Earned Value Management Systems* and as appropriate to the type of requirements being performed in this TO. Not all requirements are appropriate for EVM monitoring. After award, the Government will indicate the requirements for which it wants monthly EVM statistics to be provided. A copy of the standard is available at http://global.ihs.com/. The Government expects the contractor to employ innovation in its proposed application of EVM techniques to this TO IAW best industry practices. The following EVM status information shall be included in each MSR:

a. Planned Value (PV)
b. Earned Value (EV)
c. Actual Cost (AC)
d. A cost curve graph plotting PV, EV, and AC on a monthly basis from inception of the TO through the last report, and plotting the AC curve to the estimated cost at completion (EAC) value.
e. An EVM variance analysis that includes the following:
    1. Cost variance = (EV - AC)

2. Cost Variance % = (CV/PV X 100%)
3. Cost Performance Index (CPI) = (EV/AC)
4. Schedule Variance = (EV minus PV)
5. Schedule Variance % = (SV/PV X 100%)
6. Schedule Performance Index (SPI) = (EV/PV)
7. Estimate at Completion (EAC)
8. ACcum + 1/CPI X (BAC minus EV cum)
9. ACcum + 1/CPI X SPI X (BAC minus EVcum)
10. Variance at Completion (VAC) = (BAC minus EAC) for EAC
11. Variance at Completion % + (VAC/BAC X 100%) for EAC
12. Estimate to Completion (ETC)
13. Expected Completion Date

f. Explain all variances greater than ten percent.
g. Explain, based on work accomplished as of the date of the report, whether the performance goals will be achieved.
h. Discuss the corrective actions that will be taken to correct the variances and the risk associated with the actions.

The Government will conduct an Integrated Baseline Review within 60 calendar days after Project Start, or exercise of significant TO options, or incorporation of major TO modifications. The objective of the Integrated Baseline Review is for the Government and the contractor to jointly assess areas, such as the contractor's planning, to ensure complete coverage of the TO, logical scheduling of the work activities, adequate resources, and identification of inherent risks.

H.23 TRAVEL

H.23.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Joint Travel Regulation (JTR), prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.

Travel will be reimbursed IAW the FTR and DoD JTR. Maximum use is to be made of the lowest available customary standard coach or equivalent airfare accommodations available during normal business hours. All necessary travel meeting the above criteria shall be approved in advance by the COR. Exceptions to these guidelines shall be approved in advance by the CO or the COR.

H.23.2 TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a Travel Authorization Request (**Section J, Attachment O**) for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR and/or the JTR.

Requests for travel approval shall:

a. Be prepared in a legible manner.
b. Include a description of the travel proposed including a statement as to purpose.
c. Be summarized by the traveler.
d. Identify the TO number.
e. Identify the CLIN associated with the travel.
f. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.24 TOOLS AND ODCs

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the contractor (with subsequent approval by the Government). If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the FEDSIM COR a Request to Initiate Purchase (RIP) (**Section J, Attachment Q**). If the prime contractor does not have an approved purchasing system, the contractor shall submit to the CO a Consent to Purchase (CTP) (**Section J, Attachment P**). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the COR or an approved CTP from the CO and without complying with the requirements of **Section H.25**, Commercial Software Agreements.

H.25 COMMERCIAL SOFTWARE AGREEMENTS

H.25.1 The Government understands that commercial software tools that may be purchased in furtherance of this TO and as contemplated in the Tools and ODC CLINs in **Section B.7** may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as "clickwrap" or "browsewrap" (collectively, "Software Agreements"). The parties acknowledge that the FAR clause at

12.212(a) requires the Government to procure such tools and their associated documentation under such Software Agreements to the extent such Software Agreements are consistent with Federal law.

H.25.2 In order to ensure that the Software Agreements are consistent with Federal law, the contractor shall not make any purchase contemplated in Section C of the TOR without first securing the consent of the licensor of such software tools to amend the Software Agreements IAW the Amendment clause set forth in **Section H.25.4** below. The contractor shall submit documentary evidence of such consent as part of its technical proposal.

H.25.3 The requirements of this **Section H.25.3** apply only to those commercial software tools newly purchased under this TO; they do not apply to software furnished as GFI/GFE (if any). Further, they apply only to those Software Agreements that define the Government as the licensee or are intended to be transferred or assigned to the Government, with the Government becoming the licensee, at the end of this TO.

H.25.4 As used in the Amendment clause, the term "this Agreement" refers to each Software Agreement. The relevant definitions and the capitalization of terms (e.g., Licensee, Licensor, Software, Agreement) may be adjusted as necessary to match the nomenclature of the Software Agreement.

Amendment

For Federal Government Licensees, this Agreement is hereby amended as follows:

1. ***Dispute resolution and governing law****:* Any arbitration, mediation or similar dispute resolution provision in this Agreement is hereby deleted. This Agreement shall be governed by and interpreted and enforced IAW the laws of the United States of America, and dispute resolution shall take place in a forum, and within the time period, prescribed by applicable federal law. To the extent permitted by federal law and then only to the extent not pre-empted by federal law, the laws of the state specified in this Agreement (excluding its choice of law rules) will apply. No equitable or injunctive relief, and no shifting of legal fees or costs, may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.
2. ***Indemnification***: Any provisions in this Agreement requiring any Federal Government Licensee to indemnify any party are hereby deleted and shall not apply. Any provisions requiring the licensor to indemnify the Federal Government Licensee shall be revised to state that such indemnification, and the conduct and/or settlement of any applicable proceedings, shall be subject to 28 USC 516.
3. ***Changes in templates***: This Agreement shall apply in the version attached hereto. Subsequent updates to or changes in the licensor's standard commercial templates for such agreements shall not be binding on the Federal Government Licensee, except by prior express written agreement of both parties.
4. ***Fees, taxes and payment:*** If the Software is licensed as part of a separate Government contract between the Federal Government Licensee and a prime contractor, the

provisions of such contract regarding fees, taxes and payment shall supersede any provisions of this Agreement regarding same. Notwithstanding the foregoing: (a) express written agreement of the Federal Government Licensee shall be required prior to (i) any extension or renewal of this Agreement or the associated fees or (ii) any change in the fees; (b) late payments shall be governed by the Prompt Payment Act and the regulations at 5 CFR 1315; and (c) no cost of collection on delinquent invoices may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.

5. ***Assignment*:** Licensor may not assign this Agreement or its rights or obligations there under, in whole or in part, except IAW the procedures set forth in FAR subparts 32.8 and/or 42.12, as applicable.
6. ***No waiver of liability or cause of action***: Any provision requiring the Federal Government Licensee to agree to waive or otherwise not to pursue any claim against the licensor it may otherwise have is hereby deleted. Without limiting the generality of the foregoing, the parties agree that nothing in this Agreement, including but not limited to the limitation of liability clauses, in any way grants the licensor a waiver from, release of, or limitation of liability pertaining to, any past, current or future violation of federal law and that no clause restricting users' statements shall be read to restrict the Federal Government Licensee's ability to pursue any course of action otherwise permitted by federal law, regulation, or policy, including without limitation making public statements in connection with any suspension or debarment action.
7. ***Audit***: Any clauses in this Agreement allowing for an audit of the Federal Government Licensee's records or information systems, or verification of its compliance with this Agreement generally, shall be subject to the Federal Government Licensee's requirements pertaining to security matters, including without limitation clearances to be held and non-disclosure agreements to be executed by auditors, badging or escorting requirements for access to premises, and other applicable requirements. Any over-use identified in an audit shall be referred to the prime contractor or the Federal Government Licensee's contracting officer (as applicable) for action. No audit costs may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.
8. ***Compliance with laws*:** The parties acknowledge that the United States, as a sovereign, is subject to the laws of the United States. Nothing in this Agreement shall be interpreted to imply consent by any Federal Government Licensee to submit to the adjudicative or enforcement power of any regulatory, administrative, or judicial authority of, or the application of the laws of, another jurisdiction. Any provision inconsistent with applicable federal law that is not listed above is hereby deemed omitted from this Agreement to the extent of such inconsistence.
9. ***Third party terms***: Any third party licensing terms associated with third-party software components or products embedded in or otherwise provided with the Software shall be deemed amended IAW sections 1-8 above.

H.26 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply. The Software Agreements referenced in **Section H.25**, amended as contemplated therein, shall be deemed to constitute such disclosure with regard to their associated commercial software tools and shall prevail over any inconsistent provision in FAR 52.227-14 to the extent of such inconsistency.

H.27 AWARD FEE

See the Award Fee Determination Plan in **Section J, Attachment E**.

H.28 CONTRACTOR IDENTIFICATION

As stated in 48 CFR 211.106, Purchase Descriptions for Service Contracts, contractor personnel shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

H.29 SAFEGUARDING SENSITIVE DATA AND INFORMATION TECHNOLOGY RESOURCES

In accordance with FAR 39.105, this section is included in this TO. This section applies to all users of sensitive data and IT resources, including awardees, contractors, subcontractors, lessors, suppliers and manufacturers.

The following GSA policies must be followed. These policies can be found at http://www.gsa.gov/directives or https://insite.gsa.gov/directives.

a. CIO P 2100.1 GSA Information Technology (IT) Security Policy.
b. CIO P 2100.2B GSA Wireless Local Area Network (LAN) Security.
c. CIO 2100.3B Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities.
d. CIO 2104.1A GSA Information Technology IT General Rules of Behavior.
e. CIO 2105.1 B GSA Section 508: Managing Electronic and Information Technology for Individuals with Disabilities.
f. CIO 2106.1 GSA Social Media Policy.
g. CIO 2107.1 Implementation of the Online Resource Reservation Software.
h. CIO 2160.4 Provisioning of Information Technology (IT) Devices.
i. CIO 2162.1 Digital Signatures.
j. CIO P 2165.2 GSA Telecommunications Policy.

k. CIO P 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (Pll).
l. CIO 2182.2 Mandatory Use of Personal Identity Verification (PIV) Credentials.
m. CIO P 1878.2A Conducting Privacy Impact Assessments (PIAs) in GSA.
n. CIO IL-13-01 Mobile Devices and Applications.
o. CIO IL-14-03 Information Technology (IT) Integration Policy.
p. HCO 9297.1 GSA Data Release Policy.
q. HCO 9297.2B GSA Information Breach Notification Policy.
r. ADM P 9732.1 D Suitability and Personnel Security.

This section shall be inserted in all subcontracts.

SECTION I – CONTRACT CLAUSES

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

I.2 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request the CO will make their full text available. Also, the full text of a provision may be accessed electronically at:

FAR website: https://www.acquisition.gov/far/

Clause No	Clause Title	Date
52.203-13	Contractor Code of Business Ethics and Conduct	(Apr 2010)
52.204-2	Security Requirements	(Apr 1996)
52.204-9	Personal Identity Verification of Contractor Personnel	(Jan 2011)
52.204.10	Reporting Executive Compensation and First Tier Subcontract Awards	(Jul 2013)
52.215-21	Requirements for Cost or Pricing Data or Information Other than Cost or Pricing Data – Modifications	(Oct 2010)
52.219-8	Utilization of Small Business Concerns	(Jul 2013)
52.223-15	Energy Efficiency in Energy Consuming Products	(Dec 2007)
52.223-16	IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products	(Dec 2007)
52.224-1	Privacy Act Notification	(Apr 1984)
52.224-2	Privacy Act	(Apr 1984)
52.227-14	Rights in Data – General	(Dec 2007)
52.227-14	Rights In Data – General Alternate II or III (Use FAR Clause (52.227-14)	(Dec 2007)
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	(Dec 2007)
52.227-17	Rights In Data Special Works	(Dec 2007)
52.227-21	Technical Data Declaration Revision and Withholding of Payment – Major Systems	(Dec 2007)
52.232-18	Availability of Funds	(Apr 1984)
52.232-20	Limitation of Cost	(Apr 1984)
52.232-22	Limitation of Funds	(Apr 1984)

Clause No	Clause Title	Date
52.232-99	Providing Accelerated Payment to Small Business Subcontractors (Deviation)	(Aug 2012)
52.232-99	Providing Accelerated Payment to Small Business Subcontractors (Deviation)	(Aug 2012)
52.239-1	Privacy or Security Safeguards	(Aug 1996)
52.244-6	Subcontracts for Commercial Items	(Dec 2013)
52.251-1	Government Supply Sources	(Aug 2012)

I.2.1 CLAUSES INCORPORATED BY FULL TEXT

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of the end of the period of performance.

(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 66 months.

(End of clause)

I.3 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

GSAM website: https://www.acquisition.gov/gsam/gsam.html

Clause No	Clause Title	Date
552.204-9	Personal Identity Verification Requirements	(Oct 2012)

Clause No	Clause Title	Date
552.232.25	Prompt Payment	(Nov 2009)
552.236-75	Use of Premises	(Apr 1984)
552.239-70	Information Technology Security Plan and Security Authorization	(Jun 2011)
552.239-71	Security Requirements for Unclassified Information Technology Resources	(Jan 2012)

I.15 DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENTS (DFARS) CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

Defense Procurement website:

www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

Or

http://farsite.hill.af.mil/

Clause No	Clause Title	Date
252.201-7000	Contracting Officer's Representative	(DEC 1991)
252.203-7000	Requirements Relating to Compensation of Former DoD Officials.	(SEP 2011)
252.203-7002	Requirement to Inform Employees of Whistleblower Rights	(JAN 2009)
252.203-7003	Agency Office of the Inspector General	(DEC 2012)
252.203-7005	Representation Relating to Compensation of Former DoD Officials	(NOV 2011)
252.204-7000	Disclosure of Information	(DEC 1991)
252.204-7003	Control of Government Personnel Work Product	(APR 1992)
252.204-7004	Alternate A, System for Award Management	(FEB 2014)
252.204-7005	Oral Attestation of Security Responsibilities	(NOV 2001)
252.204-7007	Alternate A, Annual Representations and Certifications	(AUG 2014)
252.204-7012	Safeguarding of Unclassified Controlled Technical Information	(NOV 2013)
252.205-7000	Provision of Information to Cooperative Agreement Holders	(DEC 1991)
252.206-7000	Domestic Source Restriction	(DEC 1991)
252.209-7001	Disclosure of Ownership of Control by the Government of a Terrorist Country	(JAN 2009)

SECTION I – CONTRACT CLAUSES

Clause No	Clause Title	Date
252.209-7002	Disclosure of Ownership or Control by a Foreign Government	
252.211-7007	Reporting Government-Furnished Property	(AUG 2012)
252.216-7005	Award Fee	(FEB 2011)
252.223-7004	Drug-Free Work Force	(SEP 1988)
252.227-7013	Rights in Technical Data - Noncommercial Items	(Mar 2011)
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	(Mar 2011)
252.227-7016	Rights in Bid or Proposal Information	(Jan 2011)
252.227-7019	Validation of Asserted Restrictions - Computer Software	(Jun 1995)
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	(Jun 1995)
252.232-7010	Levies on Contract Payments	(DEC 2006)
252.239-7001	Information Assurance Contractor Training and Certification	(JAN 2008)
252.239-7999	Cloud Computing Services (Deviation 2015-O0011)	(FEB 2015)
252.244-7001	Contractor Purchasing System Administration	(MAY 2014)
252.245-7002	Reporting Loss of Government Property	(APR 2012)
252.245-7003	Contractor Property Management System Administration	(APR 2012)
252.245-7004	Reporting, Reutilization, and Disposal	(MAY 2013)
252.246-7001	Warranty of Data	(Dec 1991)

SECTION M – EVALUATION FACTORS FOR AWARD

J.1 LIST OF ATTACHMENTS

Copies of the following attachments will be provided electronically either as .pdf files or in particular cases, as editable files, with the release of the TOR.

Attachment	Title
A	COR Appointment Letter
B	Monthly Program Status Report
C	Department of Defense (DD) 254
D	Incremental Funding Chart (Attached at award)
E	Award Fee Determination Plan (AFDP)
F	Reserved
G	Acronym List
H	Problem Notification Report
I	Deliverable Acceptance-Rejection Report
J	Excel Workbooks – Labor CLIN Backup Documentation
K	Project Staffing Plan Template (To be removed at TOA)
L	Key Personnel Qualification Matrix (To be removed at TOA)
M	Offeror Q&A Template (To be removed at TOA)
N	Corporate Experience Sample Template (To be removed at TOA)
O	Travel Authorization Template
P	Consent to Purchase Template
Q	Request to Initiate Purchase Template
R	Corporate Non-Disclosure Agreement (NDA) Form
S	G6 Organizational Chart
T	IMN Organizational Chart
U	GuardNet Topology Diagram
V	GFE Inventory List (hardware and software)
W	ITSM Roadmap V2
X	Enterprise IT Services and Support Portfolio
Y	Draft JIE Implementation Plan
Z	Service Level Agreements (SLAs)/Service Level Targets (SLTs) April 2015
AA	PLN-3016-(U) GuardNet XXI COOP Plan v4
BB	List of ARNG Support Contractors
CC	GuardNet Services Primary and Alternate Locations
DD	EOSS Service Catalog Framework V1.0
EE	GuardNet Configuration Items
FF	ARNG State Service Levels
GG	Historical Service Statistics and Metrics
HH	January 2015 Incident Tickets
II	ARNG-2015-CTO-030 DIACAP to RMF
JJ	Current Government-Furnished Equipment and Government-Furnished Software Maintenance Agreements
KK	Historical List of Touch Labor Support and Materials
LL	COCO Facility Criteria
MM	Transition-in SLAs/SLOs

CLIN	CLIN TYPE	ESTIMATED COST	ESTIMATED AWARD FEE	TOTAL ESTIMATED	FUNDED COST	FUNDED AWARD FEE	TOTAL FUNDED
0001	LABOR						
0002	LABOR						
0004	TRAVEL						
0005	TOOLS						
0006	ODCs						
SUB							
1001	LABOR						
1002	LABOR						
1004	TRAVEL						
1005	TOOLS						
1006	ODCs						
SUB							
2001	LABOR						
2002	LABOR						
2004	TRAVEL						
2005	TOOLS						
2006	ODCs						
SUB							
3001	LABOR						
3002	LABOR						
3004	TRAVEL						
3005	TOOLS						
3006	ODCs						
SUB							
4001	LABOR						
4002a	LABOR						
4002b	LABOR						
4002c	LABOR						
4004	TRAVEL						

4005	TOOLS	(b) (4)	
4006	ODCs		
SUB			
TOTAL		(b) (4)	$ 16,390,000